PARLIAMENT
OF THE REPUBLIC OF SOUTH AFRICA

COMMITTEES
PO Box 15 Cape Town 8000 Republic of South Africa
Tel: 27 (21) 403 2597 Fax: 27 (21) 403 3205
www.parliament.gov.za

Draft Report of the Select Committee on Security and Justice on the Cybercrimes Bill [B 6B – 2017] (National Assembly – sec 75) (introduced as Cybercrimes and Cybersecurity Bill [B 6 – 2017]), dated 11 June 2020:

The Select Committee on Security and Justice, having deliberated on and considered the subject of the **Cybercrimes Bill [B 6B – 2017] (National Assembly – sec 75) (introduced as Cybercrimes and Cybersecurity Bill [B 6 – 2017])**, referred to it on 27 November 2018 and after revival in the Council on 17 October 2019, referred to the Committee on 31 October 2019 in the Council Order Paper and classified by the JTM as a section 75 Bill, reports that it has agreed to the Bill and reports as follows:

1. Background

The Cybercrimes Bill [B 6B – 2017] (National Assembly – sec 75) seeks, amongst other matters, to: create offences which have a bearing on cybercrime; criminalise the distribution of data messages which are harmful and to provide for interim protection orders; further regulate jurisdiction in respect of cybercrimes; further regulate the powers to investigate cybercrimes; further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime; provide for the establishment of a designated Point of Contact; further provide for the proof of certain facts by affidavit; impose obligations to report cybercrimes; provide for capacity building; and provide that the Executive may enter into agreements with foreign States to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes.

- The Bill is tagged as a Bill to be dealt with in terms of Section 75 of the Constitution (a bill not affecting provinces).
- The Departments reported that there would not be significant financial implications associated with the Bill to the State. The financial implications relate to the training of judicial officers and prosecutors. The SAPS has implemented a

training course for first responders in the investigation of offences which have a cyber-element.

- The Bill was referred to the 5th Parliament Select Committee on Security and Justice on 27 November 2018.
- The 5th Parliament Select Committee advertised the Bill for public comment on electronic platforms from 4 February 2019 with a deadline for written comments of 8 March 2019.

- The Bill lapsed at the end of the 5th Parliament.
- The 6th Parliament National Council of Provinces passed a resolution on 17 October 2019 reviving, amongst others, the Bill and further, that the proceedings on these Bills should resume at the stage at which they were at the end of the term; and that where Committees have commenced with the processing of the Bills, work related to the Bill would be accepted as having being done by Committees.

2. Public participation process on the Cybercrimes Bill [B 6B – 2017] (National Assembly – sec 75)

The 5th Parliament Select Committee advertised the Bill for public comment on Parliament's electronic platforms from 5 February 2019 with a deadline for written comments on 8 March 2019.

3. Summary of Submissions (See Annexure A):

- Fourteen (14) submissions were received on the Bill; including the following:
- Media Monitoring Africa (MMA)
- The Commission for Gender Equality (CGE)
- The Centre for Applied Legal Studies (CALS)
- Consolidated Submission (containing submissions from Motovantage, FNB, RMB, Wesbank, Direct Axis, Ashburton Investments)
- Jordan Griffiths
- Telkom

- Michalsons Attorneys
- Richard Ryan
- Vodacom
- Freedom of Religion (FOR SA)
- MTN
- Rachel Mazibe
- JP Morgan Chase Banking
- Anonymous Submission

4. Committee consideration of the Cybercrimes Bill [B 6B – 2017] (National Assembly – sec 75)

The 5th Parliament Select Committee received a briefing on the Bill on 5 February 2019 and thereafter advertised the Bill for written comment. The 6th Parliament Select Committee received a briefing on the Bill from the researcher and the summary of written submissions from the Content Advisor on 8 October 2019. The Select Committee received a briefing from the Department of Justice and Constitutional Development On 9 October 2019. The Select Committee invited stakeholders that provided substantive comments to make oral presentations and hosted public hearings on 12 and 13 November 2019. Vodacom and the First Rand Bank consolidated group indicated that an oral presentation would not be necessary as their written submissions outlined their concerns sufficiently. The Select Committee considered all stakeholders written submissions and the oral submissions made at the hearing.

The following organisations accepted the invitation to participate in the public hearings:

1. Telkom
2. Michalsons Attorneys
3. Media Monitoring Africa
4. Commission for Gender Equality (CGE).
5. MTN
6. Centre for Applied Legal Studies (CALS)

7. Freedom of Religion South Africa (FOR SA)

On 5 February 2020 the Department of Justice and Constitutional Development presented its response to the submissions made. The South African Police Service also responded to the public comments made on the Cybercrimes Bill and proposed further amendments to the Bill. The National Prosecuting Authority (NPA) indicated their concerns were catered for by the proposed amendments.
The Select Committee requested that the different Departments who may be affected by the provisions in the Bill meet to discuss their differences and find common ground before the next meeting.

On 11 March 2020, the Committee received a further briefing from the Department on the proposed amendments. At this meeting, the Committee agreed that the proposed amendments be referred to the parliamentary legal team for further processing and engagement with the Department.

On 10 June 2020 the parliamentary legal advisor presented the proposed amendments for consideration.

5. Proposed Amendments agreed to

The Committee considered and approved the recommendations for the amendment of the Bill as set out in Annexure B.

These recommended amendments mainly focus on-
(a) altering the tone of the Bill to reflect non-binary language as required by considerations of gender-neutrality, equality, dignity and identity;
(b) the restructuring of clause 16 to specifically reflects the impact of the paragraph (a) considerations in criminalising the disclosure of data messages of intimate images;
(c) on recommending the amendment of clauses 1, 2, 3, 11, 13, 20, 21, 22, 24, 32, 33, 39, 40, 41, 42, 44 and 59 following comments received during public hearings, as well as further engagement with the Department of Justice, SAPS and the NPA;

(d) consequential amendments following the paragraph (b) amendments throughout the provisions and the Schedule; and

(e) additional style and technical amendments throughout the text to improve readability and interpretation of the Bill.

6. Certification of the Bill

The Committee certifies that –

(i) all amendments are constitutionally and procedurally in order within the meaning of joint rule 161; and

(ii) no amendment affects the classification of the Bill.

7. Recommendation

The Select Committee on Security and Justice, having considered the **Cybercrimes Bill [B 6B – 2017] (National Assembly – sec 75) (introduced as Cybercrimes and Cybersecurity Bill [B 6 – 2017]),** referred to it on 27 November 2018 and after revival in the Council on 17 October 2019, referred to the Committee on 31 October 2019 in the Council Order Paper and classified by the JTM as a section 75 Bill, recommends the Council pass the Bill subject to proposed amendments.

Report to be considered.

Annexure A

SUMMARY OF SUBMISSIONS

CYBERCRIMES BILL

[B6B-2017]

The bill was advertised for comment on electronic platforms from 5 February 2019 to 8 March 2019.

Fourteen (14) submissions were received on the Bill; including the following:

1. Media Monitoring Africa (MMA)
2. The Commission for Gender Equality (CGE)
3. The Centre for Applied Legal Studies (CALS)
4. Consolidated Submission (containing submissiions from Motovantage, FNB, RMB, Wesbank, Direct Axis, Ashburton Investments)
5. Jordan Griffiths
6. Telkom
7. Michalsons Attorneys
8. Richard Ryan
9. Vodacom
10. Freedom of Religion
11. MTN
12. Rachel Mazibe
13. JP Morgan Chase Banking
14. Anonymous Submission

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
Definitions	**Media Monitoring Africa**	MMA submits that the Cybercrimes Bill should include a provision under the "Definitions and interpretation" in section 1 of the Cybercrimes Bill, along the following lines: **DEFINITIONS AND INTERPRETATION** **…** **(3) In undertaking any measure in terms of this Act, the State must at all times respect, protect, promote and fulfil the rights in the Bill of Rights, both online and offline, including the rights to freedom of expression, access to information and privacy, and nothing in this Act should be interpreted or relied up to unjustifiably impede the free flow of information.**
	CGE	**Definitions** **Definition of a minor.** The CGE recommends that the definition of a minor as defined in the Children's Act be included in the Bill. The Children's Act defines a child to be any person under eighteen years of age. **Definition of cyberviolence** Cyberviolence includes, but is not limited to: cyber stalking, nonconsensual pornography (or 'revenge porn'), gender-based slurs and harassment, 'slut-shaming', unsolicited pornography, 'sextortion', rape and death threats, 'doxing', electronically enabled human trafficking, any electronic communication relating to rape or death. Definitions may also be given for the acts that constitute cyberviolence.
	Jordan Griffiths	**Cyber terrorism** Part 1 of the bill does not make an attempt to define cyber terrorism as a potential crime. Cyber terrorism is a growing concern globally and considering its risks to the country it is worth considering if it should be reflected specifically in the legislation. Section 11 titled "Aggravated offences" may cover some of the crimes committed by cyber terrorists but not all of them. For instance, the use of the internet to recruit individuals to join classified terrorist organisations, the sharing and coordination of plans to conduct a

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		terror attack, or the provision of material to conduct terror attack, i.e bomb-making plans. If it is found that a person who is engaged in cyber-crime is in fact a member of an acknowledged terrorist organization and is using the proceeds of that cyber-crime to either plot or fund a cyber- attack whether it be in South Africa or abroad this should possibly be addressed as a separate and potential unique type of crime.
	Telkom	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
	Michalsons Attorneys	It must be noted that the exception in section 1(2) only addresses the unlawful processing which meets the requirements of a cybercrime in the Bill, and is also be considered unlawful processing of personal data in terms of the POPI Act. It does not take into account the processing of data outside of the POPI Act. Lastly, there is still a great concern for public officials in relation to the cybercrimes. Public officials may only act if the law has given them the power to do so. If they do something not in accordance with a law, they would be guilty of an offence. Current drafting of the cybercrimes in the Bill, does not adequately address this concern. **Suggested amendments to section 1(2) of the Bill** (2) For purposes of section 2, 3(2) or (3) or 7(1) or (2), **3, 5 or 7,** any failure to comply with— (a) the conditions for lawful processing of personal information referred to in Chapter 3; (b) section 72; or (c) the provisions of a code of conduct issued in terms of section 60, of the Protection of Personal Information Act, 2013, must be dealt with in terms of Chapter 10 of that Act.
	Consolidated Submission **(Motovantage,**	The definition of data message in the Bill is not in line with the definition of data message as defined in the ECT Act. The definition of data message in the ECT Act is used as the common

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
	FNB, RMB, Wesbank, Direct Axis, Ashburton Investments)	definition for this term when used in other legislation/regulations such as the POPIA Regulations. Consider alignment with the Electronic Communications and Transactions Act. This would ensure harmonisation of various pieces of legislation and would prevent legal interpretation difficulties. Section 1: Definition of "publicly available data" The Protection of Personal Information Act (POPIA) refers to personal information contained in a public record and personal information intentionally made public by the data subject (or in the event of a child, made public with the permission of the competent person – like a parent or guardian). This limits the scope of "publicly available data" to that personal information which is contained in a public record held by a public body or personal information made public by the data subject self. The definition in the Bill is much broader than envisaged by POPIA and the intention of the legislature should be confirmed as this will lead to misalignment. Section 1(2) It is noted that the Bill deals with "data" and not "personal information". "Data" has a broader scope than "personal information" and therefore the Bill would have a wider impact than POPIA. Was this the intention?
Chapter 2: Part 1 **Section 2**	**Consolidated Submission**	This clause will criminalise the processing (in the form of "access") of personal information if the access is unlawful in terms of POPIA (therefore there is no lawful justification for the access). However, the requirement of intent will have to be met. I am assuming that intent is limited to *mens rea* that is the intention or knowledge of the wrongdoing and that error or negligence would be excluded.
Section 2(1)	**Richard Ryan**	Chapter 2 **Unlawful access** 2. (1) Any person who unlawfully and intentionally accesses—

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		(a) data; (b) a computer program; Etc etc In my view the word intentionally accesses adds another onus of proof, in the IT world a person who unlawfully access a part of a system may "unintentionally" gain access to another part of a system, application, e.g. a mechanism of pass through authentication may allow access to a greater set of data or a different part of the network or indeed even another organisation, which may prove far more devastating. Therefore, in my opinion even though the secondary consequences caused is unlawful one could argue it was not intentional. A Prosecutor may find it impossible to prove intentional access in this circumstance.
Section 3(1)	**Consolidated submission**	We would propose that "electromagnetic emissions" should be defined. I could not locate a definition in the Electronic Communications and Transactions Act. There is also not a definition in the Electronic Communications Act. There is also no definition in RICA. This provision would also be relevant from a POPIA perspective. It is not clear whether location data would be included – for example, the location of a mobile device which is transmitted. The legislature should make its intent clear with a definition.
Section 3(3)	**Consolidated Submission**	This section sets out that if any person is found in possession of data and it is reasonably suspected that such data was unlawfully intercepted, such person is required to provide a satisfactory explanation in terms of the data possession, failing which they will be guilty of an offence. The presumption of "innocent until proven guilty" finds no application in this provision, and instead provides for an onerous requirement on the person who holds the data. It is proposed that the presumption of "innocent until proven guilty" be considered and applied here
	Vodacom	**Unlawful interception of data** Clause 3(3) of the Bill provides that – "any person who is found in possession of data, in regard to which there is a reasonable suspicion

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		that such data was intercepted unlawfully as contemplated in subsection (1) and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence". It should be noted that the Bill fails to provide an explanation of what a "satisfactory exculpatory account of possession" could entail. Particularly where there is a new category of offence, the uncertainty and ambiguity may lead to undue arrests and infringement of individuals personal rights. This is contrary to the rule of law.
Section 2(1), 2(2), 3(3)	**Freedom of Religion**	**Submit that these clauses criminalises whistleblowers and journalists.** Our concern with these clauses is that one could potentially be guilty of an offence simply for being unable to provide a satisfactory explanation for possessing certain data. This poses a massive risk to freedom of expression for especially the press and media, which is quintessential for an open and transparent democratic society. In the circumstances, we recommend the inclusion of a public interest defence.
Section 4(1)	**Anonymous Submission**	Clarity is sought on the clause regarding the '*unlawful acts in respect of software or hardware tool'* as it applies to penetration tests carried out in financial institutions for the purposes of testing the resistance of its systems Chapter 2 Part I: Clause 4(1) Any person who unlawfully and intentionally— (a) uses; or (b) possesses, any software or hardware tool for purposes of contravening the provisions of section 2(1), 3(1), 5(1), 6(1) or 7(1)(a) or (d), is guilty of an offence. Penetration testing is an important method to determine how resistant an institution's technical infrastructure is to an external attack and to test the vulnerability of its systems. This is carried out as a mandated security audit where permission is given to the penetration tester. Will guidance be provided regarding the use of penetration testing for the reasons provided above and is this excluded for purposes of this section in the Bill?

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
	Richard Ryan	**Unlawful acts in respect of software or hardware tool** 4. (1) Any person who unlawfully and intentionally— (a) uses; or (b) possesses, any software or hardware tool for purposes of contravening the provisions of section 2(1), 3(1), 5(1), 6(1) or 7(1)(a) or (d), is guilty of an offence. If I were to procure my hacking software legally (and use it to break into a company system, I am not contravening this act because the test is both UNLAWFULLY AND INTENTIONALLY) and I may well be using my lawful obtained software for legal purposes Many of these "*Hacking tools*"" and other instruments to intercept data can be legally purchased, expressly the for the purposes of hardening and testing networks and applications, many such applications and tools are provided for the express purpose of testing security of the IT systems and are licenced as such. Many security companies make a living out of accessing on the web, databases of published USERNAMES and passwords that have already been exposed, this information is used for the express purposes of heightening awareness and improving security. I am concerned that this bill may inadvertently push this information back into the hands of only the criminals, as the security organisations may be reluctant to divulge or use the information to educate and harden systems. Please also think of covering a scenario that when a system/program vulnerability is discovered it would be illegal to sell or divulge this information to anyone other that the legal owner of the system or software.
Section 5	**Consolidated Submission**	It is again important that intent is linked to *mens rea* and would exclude error or negligence. As a person could in error or negligently delete data without intentionally acting unlawfully.
Section 6	**MTN**	There is a lack of clarity on what constitutes unlawful interference, this provision can give rise to inadvertent offences for interferences in the ordinary course of system maintenance, upgrades, testing,

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		etc.
Section 7(3)(i)	**Consolidated Submission**	The term 'financial transaction' has not been defined. Define "financial transaction" to ensure clarity in interpretation
Section 10	**CALS**	**Balancing of Rights** Various cultures and religions have practices that may be manipulated and become a form of online abuse. Furthermore, unwanted consequences of taking part in the various practices may not always be communicated to the potential victim In light of this the Bill will need to balance the right to certain cultural practices (section 15 and section 30 of the Constitution) with right of vulnerable individuals to protection of their dignity (section 10 of the Constitution) as well as their right to safety and security (section 12 of the Constitution) as an individual. INTERPOL draws a useful distinction between 'cybercrime' on the one hand and 'cyber-enabled crime' on the other. 'Cybercrime' is a term used to refer to crimes that are by nature technological and involve attacks on computers, while 'cyber-enabled crimes' are existing crimes which are now taking place using online media like child pornography. We would propose adopting a similar approach and restricting the Cybercrimes Bill to 'cybercrimes' while adapting existing legislation to incorporate 'cyber-enabled crimes'. Should the above approach prove unfeasible, we would recommend that several of the sections be amended to be as inclusive as possible. 3.2.1. Section 10 should be amended to include a specific reference to extortion for sex acts and be included as a sexual offence with a corresponding stronger sentence imposed.
	CGE	**Section 10: Cyber Extortion** Cyber extortion as described in section 10 must be expanded to include extortion or blackmail through revenge porn / non-consensual pornography or sharing of intimate images. This concept is known as sextortion. Cyber extortion as a concept should not only focus on unlawful acquiring of data, the interference with data, data storage or programming,

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		passwords and access codes, but also look at sextortion.
	Consolidated Submission	Section 10(i) the word 'advantage' should be expanded on in definitions section, this could be monetary gain or using the unlawful data to influence a certain outcome.
Section 11(1)(b)	**Consolidated Submission**	Many computer systems, data storage systems etc in an organization may be outsourced or under control of a third party and may not be exclusively used by the financial institution. Recommendation: a) **"restricted computer system"** means any data, computer program, computer data storage medium or computer system under the control of, or used at the instruction of or exclusively **[used]** by— (i) any financial institution; or…
Section 11(2)(a)-(g)	**Consolidated Submission**	Subsections are too broad, e.g. "essential service, facility or system", essential to who or for what is not explained. These subsections are left open for interpretation which is concerning since the section deals with aggravated offences. Where reference is made to "any person" an insertion of "excluding electronic communications network service providers" be added.
Section 11(2)(e)	**Consolidated Submission**	Major economic loss has not been defined in the Bill. We suggest adding the following: Measurement, criteria, definition and what would constitute major financial loss. Define 'major economic loss"
Section 11	**CGE**	**Section 11: Aggravated offences** Section 11(2) refers to various instances where a person may be guilty of an aggravated offence. The CGE submits that a person that infringes on the dignity and privacy, as well as the mental and emotional integrity of a person may be found guilty of an aggravated offence. The CGE therefore proposes a sub-section, to read: (2) Any person who commits an offence referred to in section 5(1),

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		6(1) or 10, which – …(h) violates the dignity or privacy of any person, or any number of persons; …(i) causes mental and emotional harm to a person, or any number of persons
Section 12	**CALS**	Section 12 should likewise be amended to include specific reference to theft of sexualised or "intimate images" and/or sound and/or video and/or text and be included as a sexual offence with a corresponding stronger sentence imposed.
Chapter 2: Part II **Section 14**	**Consolidated Submission**	It is provided under this section that "any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which: • Incites damage to property or violence (S14) • Is of an intimate nature without the person's consent. Is guilty of an offence. FNB could be held criminally liable for inciting violence when our part would simply be providing an electronic platform. Where reference is made to "any person" an insertion of "excluding electronic communications network service providers" be added. Alternatively, define any "person" to the exclusion of electronic communications network service providers.
	CALS	Section 14 should be amended to account for any unwanted messages of a sexual nature and included as a sexual offence.
	Freedom of Religion	Clauses 14 & 15 (under Part II) are unnecessary in light of the existing legislation and existing legal remedies (such as interlocutory relief, damages claims for defamation and/or economic harm) which can be employed to prevent or sanction malicious communications. Recommends that Clause 14 and 15 be deleted from the Bill.
Section 15	**Consolidated Submission**	It is provided under these sections that "any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which: • Threatens damage to property or violence(S15) • Is of an intimate nature without the person's consent, Is guilty of an offence.

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		Electronic Communications Network Service Providers could be held criminally liable for inciting violence when their part would simply be providing an electronic platform The current wording refers to “any person”. This is open for interpretation. Whilst the customers may initiate distribution the prohibited data messages, the function of distributions occur on a telecommunication network. Electronic communications network service providers may be deemed to be “any person” under the current wording. Where reference is made to “any person” an insertion of “excluding electronic communications network service providers” be added. Alternatively, define any ‘person’ to the exclusion of electronic communications network service providers.
	CALS	Section 15 should likewise be amended to account for any unwanted messages of a sexual nature and included as a sexual offence. It should also incorporate threats to release content such as that contemplated in section 16.
Section 16	**Consolidated Submission**	Section 16(1) Consent can be both verbal and written how would one prove consent was granted prior to the distribution of the image Section 16(2)(a) We would propose that the legislature consider the definition of ‘de-identify’ in section 1 of POPIA to determine whether a person can be identified in an image. Therefore, we would propose alignment with POPIA to determine whether a person is identifiable or not.
	CALS	Section 16 should be broadened to include sexualised or “intimate images” as well as sound and/or video and/or text. It should also be amended to remove mentions of “a female” and rather include any kind of data message which the complainant subjectively identifies as sexualised.
	CGE	**Section 16: Data message which incites damage to property or violence** The CGE supports clause 16, but submits that acts of cyber violence as submitted under the definitions should resort under clause 16, with specific reference to the recording of sexual violence and rape on social media platforms and other electronic and online

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		means. Online human trafficking should also be addressed in section 16 as an intention to incite violence and harm against a person or a group of persons.
Section 17	**Consolidated submissions**	By providing the electronic platform, Electronic Communications Network Service Providers might be implicated in the aiding and abetting of a crime. Where reference is made to 'any person' an insertion of 'excluding electronic communications network service providers' be added. Therefore, the wording should be changed to be less ambiguous in this regard. Alternatively, define any 'person' to the exclusion of electronic communications network service providers.
	CGE	**Section 17: Data message which is harmful** The CGE supports clause 17, and submits that the concepts of cyber harassment and cyber stalking should be included in section 17. The CGE therefore submits that section 17(2) should read: (2) for the purpose of subsection (1), a data message is harmful when- ……. (e) cyber harassment or cyber stalking which is of a sexual nature are taking place by using data messages, computer system or broadcasting systems.
	MMA	With regard to **sections 17 and 18** of the Cybercrimes Bill, MMA proposes inserting the word "imminent" before all references to violence, to appropriately narrow the causal nexus between the exercise of speech and the resultant harm that the Cybercrimes Bill seeks to address.
Section 18	**Consolidated Submission**	A service provider should not be held criminally liable

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		for a platform that they have provided. Electronic Communications Network Service Providers can be held criminally liable for simply providing a platform for electronic communications. Where reference is made to "any person" an insertion of "excluding electronic communications network service providers" be added. Therefore, the wording should be changed to be less ambiguous in this regard. Alternatively, define any "person" to the exclusion of electronic communications network service providers.
	CGE	**Section 18: Distribution of data message of intimate image without consent** The CGE supports section 18 and recommends a sub-clause Section18 to read as follows: Section 18(1)(a) Any person (''A'') who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message of an intimate image of a child, is guilty of an offence, despite the consent of the child. **Defences for the proposed section 18(1)(a)** The CGE recommends the inclusion of the below sub-clause for defences against offences in terms of the proposed section 18(1)(a). It is not a valid defence to a charge under section 18(1(a)), in respect of an intimate image of a child that- *(i)* the accused person believed that data message of an intimate image of a person shown, was or was depicted as being 18 years or older unless the accused took all reasonable steps to ascertain the age of that person; and *(ii)* took all reasonable steps to ensure that, where the person was 18 years or older, the intimate image did not depict that person as being under the age of 18 years.
Section 19	**Consolidated Submission**	It is noted that the penalties consist of a fine, imprisonment or both. In the event that an organisation is found to be guilty of the commission of a cybercrime, it is unclear how much the organisation may be fined and/or who the

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		accountable person will be if imprisonment is ordered. Additionally, the Bill empowers the Courts to try offences in some instances, even if the circumstances appear to be vague. In this regard, the Bill should be more specific and should provide clear guidelines. It is requested that clarity be provided around the fines and penalties imposed on organisations and that guidelines be provided around the jurisdiction of Courts to try offences in instances with vague circumstances.
	MMA	With regard to section 19 of the Cybercrimes Bill, MMA proposes that a requirement of harm should be inserted. This is to avoid any possible unintended consequences, such as a parent who shares a nude picture of a new born baby with family members falling foul of this provision. While such an example may be unlikely to lead to a prosecution, the concern is that this may be selectively used and thereby have a chilling effect on freedom of expression Accordingly, in line with section 28(2) of the Constitution, which recognises that "[a] child's best interests are of paramount importance in every matter concerning the child", MMA proposes the insertion of a new section following section 19 under Chapter 3 of the Cybercrimes Bill, along the following lines: **BEST INTERESTS OF THE CHILD** **(1) In applying the provisions of this Act to a child, as defined in section 1 of the Child Justice Act 75 of 2008, due regard shall be had to the best interests of the child, the age and maturity of the child, and the express intention of the child.** **(2) The penalties set out in this Act do not apply to any child to whom the provisions of the Child Justice Act apply.** **(3) (a) The State has a duty to promote awareness amongst children, educators, parents, guardians and other relevant persons of the provisions of this Act, and other related matters of cyber policy.** **(b) Without derogating from the general nature of this duty, the Interdepartmental Steering Committee, in conjunction with the Cabinet members responsible for the administration of justice, communications, basic education, and higher education and training, must undertake the following:** **(i) Conduct education and information campaigns; and**

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		(ii) Ensure that all public officials who may be involved in the investigation and prosecution of offences under this Act are educated, informed and sensitised to the appropriate application of this Act to children.
	CALS	Section 19 (7) states that '[a]ny person who contravenes section 14, 15 or 16 is liable on conviction to a fine or to imprisonment for a period not exceeding three years or to both a fine and such imprisonment'. In instances of online sexual violence, no sentence should result in a mere fine. Although a fine is an option for certain sexual offences as set out under section 56A in SORMA, this is an incorrect approach to dealing with sexual violence offences. In light of the comparable harm, all sexual offences should be treated as serious sexual offences and be added to the list of offences that attract minimum mandatory sentencing as set out under section 51 of the Criminal Law Amendment Act 38 of 2007. Section 19 (7) should be amended to have the option of a fine removed for those convicted of a sexual offence.
	CGE	**Section 19: Order to protect complainant pending finalisation of criminal proceedings** The CGE supports section 19 that highlights the aggravating factors to be considered for imposing a sentence and recommends the following additional aggravating factors to be included: (a) The fact that the depiction of the intimate images was of child or children; (b) The fact that and the extent to which minor children have been exposed to the intimate images; (c) The fact that the depiction of the intimate images was of persons who are mentally disabled; (d) The fact that and the extent to which persons who are mentally disabled have been exposed to the intimate images
Section 20	**Consolidated Submission**	**Section 20(1)(a)** This section provides for a complainant to lay a charge with the SAPS on the allegation of a malicious

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		communications offence committed against them; such person may apply to Court ex parte for an order prohibiting any person from further making available, broadcasting or distributing the data message. It is submitted that in some instances the alleged offender may also incite and/or encourage other persons to make the data message further available. It is recommended that this section specifically provide for a prohibition against such instances. It is proposed that the subsection be reworded as follows "… prohibit any person from further making available, broadcasting or distributing the data message and/or prohibit any person from inciting and/or encouraging other persons to further make available, broadcast or distribute the data message…". Section 20(1)(b) and Section 22 (2)(c) Order an Electronic Communications Service Provider "ECSP" to remove or disable access to the data message in question Practical implication of implementing such functionality to remove or disable access may not be possible. This may be observed where a user transmits a message to another user in another network. Also, the question here would be should access of all the distributed parties be removed/ disabled?
	CALS	Section 20 (1) should be amended to remove reference to the finalisation of the order to be dependent on separate criminal proceedings. Section 22 (1) should likewise be amended.
	Vodacom	Further, Vodacom submits that the provision of clause 20(1)(b) would not be effective because social media platforms or normal multi-media messaging services could be used to commit the offence which would mean that such messages become self-propagating. Unless the source of the message can be determined, this provision could be applied punitively or in error. Clause 20(1)(b) only makes reference to a computer system and not computer storage medium or computer program which in Vodacom's view should be included.
Section 21	**MTN**	Section 21 information should be provided taking into account an individual's constitutional right to privacy,

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		right to dignity as well as freedom of expression.
Section 22	**CGE**	**Section 22: Penalties** The CGE supports the provisions of section 22, but submits that a register for offenders should be established in respect of offences relating to cyber-violence and sexual offences. The register should have the same functionality and purpose as the Register prescribed by the Children's Act. It is therefore submitted that section 22 should read: (1) Any person who contravenes the provisions of section 16, 17 or 18 is liable on conviction to a fine or to imprisonment for a period not exceeding three years or to both a fine and such imprisonment. The person who contravenes the said provisions' details will be captured in a register in respect of cyber-violence and sexual offences.
	Vodacom	Vodacom, however, welcomes the inclusion of 22(6)(b) which provides that whenever a person is convicted of an offence in terms of section 14, 15 or 16, the trial court must issue an order that the person must reimburse all expenses reasonably incurred by an electronic communications service provider or person in control of a computer system to remove or disable access to the data message in question.
Section 23	**MMA**	Accordingly, in similar terms to the public interest override contained in the Films and Publications Act 65 of 1996, MMA proposes the inclusion of an additional sub-section to the current section 23 under the heading "Penalties", along the following lines: **PENALTIES** **…** **(3) The penalties contained in this Act do not apply when, judged in context, and except with respect to child pornography, the publication is a bona fide documentary, or is a publication of scientific, literary, artistic, or satirical merit, or is on a matter of public interest, or is already in the public domain.**
Section 24	**Consolidated Submission**	Section 24(6) This section provides for the National Commissioner and the National Head of Directorate, in consultation with the National Director of Public Prosecutions, to

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		issue directives which all SAPS officials are obliged to comply with in the execution of their functions in terms of the Act, insofar as it relates to investigating offences committed outside of the Republic. It is unclear what the consequences will be if a SAPS official fails to follow these directives and where such failure results in a monetary loss to a company and/or failing to secure a conviction. It is also unclear what recourse the company would have if, for example, it suffered monetary loss due to the negligence of the SAPS official in failing to follow the directives in the course and scope of the investigation. It is requested that guidance be provided around the consequences for a SAPS official in failing to comply with the directives especially where such failure leads to monetary loss for a company and/or failure to secure a conviction. Additionally, it is requested that guidance be provided around the recourse companies may have in the event that they suffer monetary loss due to the failure of a SAPS official to comply with the issued directives
Section 25	**MTN**	Section 25 – MTN is concerned about the extensive seizure powers granted to the State through the Bill. MTN submits that the limitations need to be specified in the warrant and such limits should only be confined to access control inter relating to the network of the ECSP.
Chapter 4: Section 26(1)	**Consolidated Submission**	This section empowers various designated parties to issue standard operating procedures which must be observed by SAPS officials and any other person/agency authorised to assist with an investigation. The standard operating procedures must be issued within 6 months of this Chapter becoming effective and must follow a consultative process. The principle of issuing standard operating procedures is supported, however it is important that these procedures be clear, practical, effective and that clear consequences for non-compliance be stipulated. This should be rolled out with adequate training. It is important for role players to understand their obligations, to comply with their obligations and to be aware of the consequences of non-compliance. This would play a significant role in instances where convictions fail to be secured due to, for example, inadmissible evidence due to mishandling of evidence. It is proposed that the standard operating procedures

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		be clear, practical and effective and that it be supported by a rigorous and adequate training programme. Additionally, all impacted officials should be fully aware of their obligations, their failure to comply and the consequences of non-compliance, which should include negligence.
	Telkom	Telkom would like to emphasise the importance of clear Standard Operating Procedures to clarify the obligations. 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.
	MTN	Proposes that Section 26 take into consideration: 1. That no action should impair the function of a computer or storage media 2. That no action should produce the effect of disrupting the service of an electronic communications service provider (ECSP) to its customers not implicated in the offence or reducing service quality to such persons 3. No action taken should risk the disclosure of personal information or confidential information of any ECSP customer not implicated in the offence. 4. No action taken should produce a limitation on the rights of customers to object to the preservation or disclosure of data provided for in other existing laws. 5. No action taken should unduly impose financial costs and business disruption of the ECSP

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
Section 27	**Consolidated Submission**	**Section 27 read with section 32(1)** It is noted that the provisions of the Criminal Procedure Act apply in addition to the provisions of Chapter 3, insofar as it is not inconsistent. This principle is supported especially insofar as it relates to the provisions around search and seizure without a warrant. This principle is supported as it would assist in achieving the objectives of the Bill.
Chapter 4 broad comments	**Consolidated Submission**	Provides investigators with far reaching powers to access (without limitation), as well as to seize, 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. There are no rights provided for a person to object to search and seizure e.g. where privileged information is involved. Such rights exist under POPIA S87. Therefore, there should be some consistency as it relates to rights to object to the search and seizure. Concern that a financial institution's data systems may contain confidential client information, commercially sensitive information, as well as privileged information, etc. Additionally, removal or rending inaccessible certain of the systems may have unintended consequences and result in breakdown of services/business interruption. Such broad ranging powers to access or seize such systems may compromise unrelated data or business activity This chapter should include provision for the controller or owner of the system/ data an opportunity to object to the accessing/seizure on various (but very limited and reasonable) grounds, which would neutralise the access to the data until a decision is made as to what limits or protocols should be applied to the access/seizure so as to place as little harm or damage to the owner/controller, as possible. The inclusion of an "objection to search and seizure" clause should align to S87 of POPIA (but perhaps extend to confidential client information and commercially sensitive information, not just privileged information). S87 of POPIA states as follows: **Objection to search and seizure** "87. *If the person in occupation of any premises in*

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		respect of which a warrant is issued under this Act objects to the inspection or seizure under the warrant of any material on the ground that it— *(a) contains privileged information and refuses the inspection or removal of such article or document, the person executing the warrant or search must, if he or she is of the opinion that the article or document contains information that has a bearing on the investigation and that such information is necessary for the investigation, request the Registrar of the High Court which has jurisdiction or his or her delegate, to attach and remove that article or document for safe custody until a court of law has made a ruling on the question whether the information concerned is privileged or not; or* *(b) consists partly of matters in respect of which those powers are not exercised, he or she must, if the person executing the warrant so requests, furnish that person with a copy of so much of the material as is not exempt from those powers."*
Section 28	**Consolidated Submission**	There are no rules regarding the execution of warrants. Such rules exist under POPIA S84. Therefore, there should be consistency as it relates to the rules for the execution of warrant. The inclusion of an "execution of warrants" clause which should align to S84 of POPIA as follows: Execution of warrants "*84. (1) A police officer who is assisting a person authorised to conduct an entry and search in terms of a warrant issued under section 82 may overcome resistance to the entry and search by using such force as is reasonably necessary.* *(2) A warrant issued under this section must be executed at a reasonable hour unless it appears to the person executing it that there are reasonable grounds for suspecting that the evidence in question would not be found if it were so executed.* *(3) If the person who occupies the premises in respect of which a warrant is issued under section 82 is present when the warrant is executed, he or she must be shown the warrant and supplied with a copy of it, and if that person is not present a copy of the warrant must be left in a prominent place on the premises.* *(4) A person seizing anything in pursuance of a warrant undersection 82 must give a receipt to the occupier or leave the receipt on the premises.* *(5) Anything so seized may be retained for as long as is necessary in all circumstances but the person in occupation of the premises in question must be given a copy of any documentation that is seized if he or*

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		she so requests and the person executing the warrant considers that it can be done without undue delay. *(6) A person authorised to conduct an entry and search in terms of section 82 must be accompanied and assisted by a police officer.* *(7) A person who enters and searches any premises under this section must conduct the entry and search with strict regard for decency and order, and with regard to each person's right to dignity, freedom, security and privacy.* *(8) A person who enters and searches premises under this section must before questioning any person— (a) advise that person of the right to be assisted at the time by an advocate or attorney; and* (b) allow that person to exercise that right. *(9) No self-incriminating answer given or statement made to a person who conducts a search in terms of a warrant issued under section 82 is admissible as evidence against the person who gave the answer or made the statement in criminal proceedings, except in criminal proceedings for perjury or in which that person is tried for an offence contemplated in section 102 and then only to the extent that the answer or statement is relevant to prove the offence charged.*
	Jordan Griffiths	**Deliberation on the Point of Contact and role of SAPS** The current implementation vehicle for this bill speaks to placing the Point of Contact within the South African Police Service. The challenge with this approach is that it essentially centralizes all cyber responsibility with the police service which may not only overwhelm the service but also be impractical in its actual implementation. Investigating individual cyber-crimes should indeed be a clear priority for the South African Police Service but what happens if there is a coordinated cyber- attack against critical national infrastructure such as the power grid, water infrastructure or transportation systems. Would this also then fall within the realm of the South African Police Service? Globally, various countries across the world have introduced Cyber Command units as part of their Defence force. They work towards supporting their respective nations in the case of cyber-attacks by acting as a cyber-defence while also ensuring that they are able to identify the culprits that are behind sustained attacks that target assets falling under the umbrella of National Security. It is somewhat unreasonable to assume that the

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		South Africa Police Service should be the sole implementing agent behind this legislation as it omits the role of critical role players such as National Intelligence and the Defence Force as a whole. Once again, I encourage the committee to engage on this matter. If there is a major cyber-crime or an act of cyber terrorism committed against the state one should ask whether or not the South Africa Police Service should have the sole responsibility for responding to it in terms of the initial investigation and response. The successful capacitation of resources within the country's security apparatus will be essential if this bill is to be effectively implemented properly. Currently the investigative capacities within SAPS to investigate cyber-crimes are largely non-existent with private sector firms usually relying on external parties to do their investigations. Although this is a matter not necessarily relevant to the bill itself, it must be emphasized that the without the necessary budget to develop the skills required to police the cyber environment this bill will fail in its aspirations. South Africa is one of the worst affected countries when it comes to cyber- crimes, a result of a society which has gone through increased levels of inter-connectivity which has outpaced our ability to provide sufficient technology literacy to our population. Leaving millions of people vulnerable when it comes to how they interact and transact online.
	Rachel Mazibe	Individual submission merely reinforcing the need to investigate and prosecute cybercrimes effectively
Section 29	**MTN**	MTN submits that the authority provision to in S29(1)(a) of the Bill to a magistrate to be able to authorize a search and seizure warrant be removed, and that the authority only vests with the "Designated Judge" as defined in RICA.
Section 34	**Consolidated Submissions**	This section places an obligation on a financial institution, amongst others, to provide "technical assistance and such other assistance as may be reasonably necessary" to a SAPS official /investigator in order to search, access or seize an article. Failure to do so will result in it being guilty of an offence and may be liable to a fine, 2 years imprisonment or both. This section is very onerous as it places an obligation on the financial institution to provide "technical" and "such other assistance" as required, without taking into account resources, capacity,

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		availability and normal day to day running of the business. Additionally, “such other assistance” as required is set out too broadly and may even be something which the financial institution is unable to provide. It may also be reasonable in certain scenarios to refuse to provide technical assistance/other assistance where the security of unrelated data is in jeopardy. The expectation on financial institutions to handover access codes, passwords, etc to highly sensitive bank systems to a police investigator on an unfettered basis is open for abuse and this power should be curtailed as far as possible. The section needs to build in a similar control as the comment to Chapter 4 above, giving the system owner or controller an opportunity to object on limited and reasonable grounds prior to handing over access codes, passwords etc or to be able to provide such assistance on a limited and controlled basis with appropriate safeguards. Alternatively, It is proposed that the section be reworded to read as “… in terms of section 29(1) should, if required, and insofar as it is reasonable and practicably possible, provide (a) technical assistance and (b) such other assistance…”.
	Vodacom	**Assisting police official or investigator** Clause 34 provides that an electronic communications service provider, financial institution and other persons, who are in control of data, a computer program, a computer data storage medium or a computer system must provide technical assistance and other assistance to a police official who is authorised in terms of a warrant to conduct an investigation, in order to search for, access and seize an article. Failure to comply can result in a conviction and a fine or imprisonment. Vodacom proposes an amendment to Clause 34(1) to include that in the instance where an article which is under the control of an electronic communications service provider, is subject to a search authorised in terms of section 27(1), such search, access or seizure should be exercised in a way which must not disrupt the services performed by an electronic communications service provider. In light of the fact that electronic communications service providers are a mere channel of transmission of information or data, Vodacom proposes the inclusion of a "mere conduit clause", specifying that

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		electronic communications service providers shall not be criminally liable for criminal actions committed on its network unless they have intentionally and unlawfully committed an offence under the Act.
Section 35	**MTN**	Section 35 – recommends that provision be made for the police official to be provided with a digital copy of the information required so as to not disrupt the daily functioning of ECSPs.
Section 39	**Consolidated Submission**	s39(2)(c) - Intent of wording may not be properly conveyed by the current drafting –as chapter 4 and 5 deal with criminal activity, in almost all instances a disclosure would be revealing criminal activity and s39 would have limited impact? Not sure of the intention, but propose the sub-section is revisited to clarify.
Section 40	**Telkom**	*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 section2 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. **Expedited Preservation Orders for Data/ Evidence** Where data preservation orders are received that carry a "Top Secret" classification, such orders can only be dealt with by individuals that have the appropriate clearance. Vodacom is concerned that it might receive preservation orders where the information requested would necessitate the involvement of individuals that do not have the prerequisite clearance levels.
Section 41	**MTN**	Section 41 provides for a form of take down of data messages. This does not take into account messages transmitted via social media sites which are not managed or under direct control of an ECSP such as MTN, it will be impossible for an ECSP to prevent the further dissemination of the data

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		message.
Section 43	**Consolidated Submission**	This section provides for the application in Section 42 to be made by way of oral application (as opposed to written application). If granted, the outcome will be that a preservation of evidence direction will be issued. However, it is unclear what maximum period applies in terms of preserving the evidence or if the 90-day period, as referenced in Section 42, applies. It is requested that clarity be provided around what maximum time period applies, in terms of the preservation of evidence and/or if the 90-day time period, as referenced in Section 42, applies.
Section 48	**Telkom**	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. 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. 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

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		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. Furthermore, when receiving preservation orders as envisaged in the Bill, electronic communications service providers might be placed in the situation that they cannot comply 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. 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

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		Cybercrimes Bill, in particular as all the directions are issues by a judge designated in terms of RICA.
Chapter 5 Section 54	**Consolidated Submission**	This section requires that a financial institution, amongst others, report to the SAPS within 72-hours of becoming aware that its computer system was involved in the commission of one of the relevant offences. Additionally, it requires that the financial institution preserve any information which may be of assistance in investigating the offence. Failure to do so will result in a guilty conviction and will lead to a fine not exceeding R50 000. However: (i) Insofar as the 72-hour reporting period is concerned, this section does not take into account that it may not always be reasonable and/or practical to report within that time period due to internal processes and/or business constraints. (ii) Insofar as the requirement for preserving any information is concerned, no time period has been provided for the preservation. It is highlighted that information cannot be held for an indefinite period and a time frame must be applied to it. It is proposed that this section builds in a process to allow for a reasonable extension of the timelines where a valid motivation can be put forward for the extension. Alternatively, (i) The 72-hour time period should be increased to 5 business days to afford the financial institution with adequate time to follow its internal processes and to ensure that it is reporting adequately and accurately. Where there are resource constraints, the time period will also enable the financial institution to make the necessary arrangements to ensure it meets its reporting obligation. (ii) Insofar as the requirement of preserving the evidence is concerned, it is proposed that a reasonable time period for preservation be applied. **S54 (1)(a) Reporting obligations and capacity building** The Bill requires that offences must be reported without undue delay, and where feasible, not later than 72 hours after having become aware of the incident There may well be instances where reporting within 72 hours is not possible whilst steps are being taken to investigate and confirm the cybersecurity incident. Moreover, there may be instances where no information relating to the incident has been preserved. For example, a cybercriminal will try to

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		"*hide their tracks*" and as a result, information relating to the incident might not be preserved as required in the Bill. The above should be confirmed with the Information Security Function. If a section like this one, which imposes very short reporting timelines, is going to prescribe a sanction, there should be an opportunity to apply for an extension of the time periods to the regulator, on reasonable grounds, especially with cybercrime where the perpetrator or cause of the offence may not be known without in-depth investigation Suggested wording is as follows: *(a) Without undue delay and, where feasible, **[not later than 72 hours]** after having become aware of the offense, report the offense in the prescribed form and manner to the South African Police Service* *Preserve any information**, if available**, which may be of assistance to the law enforcement agencies in investigating the offense.*
	JP Morgan Chase Banking	**Section 54: The 72hrs reporting timeframe seems reasonable.** While JPMorgan Chase Bank Johannesburg Bank would prefer no specific timeframe, (we prefer the requirement to report be within a reasonable amount of time after confirmation that a breach/offence occurred). The above comment would not require the firm to actively monitor its networks for evidence of a cybercrime and the 72-hour clock starts ticking only after we are aware of the offence, not when we are aware of the activity.
	Telkom	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.
	Vodacom	**Obligations of electronic communications service providers and financial institutions** In terms of clause 54 an electronic communications service provider or financial institution that is aware or

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		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: 1. 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 2. preserve any information which may be of assistance to the law enforcement agencies in investigating the offence. It is pertinent to constrain expectations on what data should be reasonably preserved. Vodacom expresses concern about the legal workload and costs to contest regular preservation orders on grounds of unreasonable expectations or substantive technical limitations. Vodacom is of the view that "any information" must be more specifically prescribed in order to cater for technical limitations and/or relevancy. Clause 54(4) provides 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: 1. Monitor the data which the electronic communications service provider or financial institution transmits or stores; or 2. Actively seek facts or circumstances indicating any unlawful activity. Vodacom submits that subject to any other law or obligation, that subsection (1) must not be interpreted to imply that the mere conveyance of a data message by an electronic communications service provider's computer system means that its computer system is involved in the commissioning of any category or class of offences provided for in Chapter 2, and/or that its conveyance equates to awareness.
Section 59	**Consolidated Submission**	We would propose the incorporation of a fair procedure in the promulgation of regulations which would include public consultation and a comment procedure.

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		We would propose the incorporation of a fair procedure in the promulgation of regulations which would include public consultation and a comment procedure.
	MTN	Regulations in Chapter 9 should also uphold the rights of the ECSPs. Therefore, Section 59(2) should be amended as follows: *"The Cabinet member responsible for policing, in consultation with the Cabinet member responsible for the administration of justice must make regulations regulating the manner in which an electronic communications service provider must report the use of its computer network or electronic communications network to commit an offence to the South African Police Services* ***on a confidential basis****."*
General Submissions **Interdepartmental Steering Committee Recommendation**	**MMA**	It remains a key concern for MMA that there is a lack of any overarching internet governance policy in South Africa. The Cybercrimes Bill will form one more in a plethora of legislation dealing with overlapping and interrelated cyber matters, and a number of bodies with similarly unclear and overlapping mandates. In turn, rather than alleviate this concern, the Cybercrimes Bill exacerbates this concern by adding a further layer of complexity, without it being fully considered how the Cybercrimes Bill coheres with existing legislation. A further constitutional consideration relates to cooperative governance and intergovernmental relations. In terms of section 41(1)(c) of the Constitution "[a]ll spheres of government and all organs of state within each sphere must provide effective, transparent, accountable, and coherent government for the Republic as a whole" and the must "co-operate with one another in mutual trust and good faith by coordinating their actions and legislation with one another". Accordingly, MMA proposes the establishment of the Interdepartmental Steering Committee on Internet Governance, to serve as a necessary – and arguably constitutionally required – central node within the state, as a response to bring harmony to South Africa's internet governance framework and to ensure swift and effective state responses to cybercrimes. Accordingly, MMA proposes the inclusion of a new section along the following lines:

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		INTERDEPARTMENTAL STEERING COMMITTEE (ISC) ON INTERNET GOVERNANCE **(1) The ISC on Internet Governance is hereby established.** **(2) The ISC on Internet Governance consists of--** **(a) a chairperson who is the Director-General: Department of Justice and Constitutional Development;** **(b) members who are the Heads of the representative Departments and one of their nominees who must be officials--** **(i) at the rank of at least a chief director or equivalent, of a representative Department, who are specifically nominated by a Head of that representative Department to serve on the ISC on Internet Governance; and** **(ii) to whom a security clearance certificate has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994);** **(c) members set out in sub-section (9).** **(3) The Cabinet member responsible for the administration of justice must appoint a member to act as chairperson whenever the chairperson is absent from the Republic or from duty, or for any reason is temporarily unable to carry out the responsibilities as chairperson.** **(4) The work incidental to the performance of the functions of the ISC on Internet Governance must be performed by a secretariat, consisting of designated administrative personnel of the Department of Justice and Correctional Services.** **(5) The objects and functions are to coordinate, rationalise and implement government policy relating to internet governance, cybercrimes and cybersecurity, to undertake educational and awareness campaigns, and to assist and advise on the formulation of future policy.** **(6) The Cabinet member responsible for the administration of justice must oversee and exercise control over the performance of the functions of the ISC on Internet Governance.** **(7) The Cabinet member responsible for the administration of justice must, at the end of each financial year, submit a report to Parliament regarding progress that has been made towards achieving the objects and functions of the ISC on Internet Governance.** **(8) For the purposes of this section--** **(a) "Head of a Department" means the incumbent of a post mentioned in Column 2 of Schedule 1, 2 or 3 to the Public Service Act, 1994, and includes any employee acting in such post; and**

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		(b) ''representative Department'' means-- **(i) the Department of Defence;** **(ii) the Department of Home Affairs;** **(iii) the Department of International Relations and Cooperation;** **(iv) the Department of Justice and Constitutional Development;** **(v) the Department of Science and Technology;** **(vi) the Department of Telecommunications and Postal Services;** **(vii) the Financial Intelligence Centre, established by section 2 of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001);** **(viii) the National Prosecuting Authority;** **(ix) the National Treasury;** **(x) the South African Police Service;** **(xi) the South African Reserve Bank;** **(xii) the South African Revenue Service;** **(xiii) the State Security Agency;** **(xiv) the Information Regulator;** **(xv) any other Department or public entity which is requested, in writing, by the Chairperson of the ISC on Internet Governance to assist.** **(9) The ISC on Internet Governance should also comprise the following members:** **(a) Two representatives from opposition parties represented in the National Assembly;** **(b) Two teachers of law, or members of the attorneys' or advocates' profession, with knowledge of internet governance laws who are approved by the Chairperson of the ISC on Internet Governance following a public call for nominations;** **(c) Two technical experts in internet governance who are approved by the Chairperson of the ISC on Internet Governance following a public call for nominations;** **(d) Two members of civil society organisations working on internet governance who are approved by the Chairperson of the ISC on Internet Governance following a public call for nominations.** **(10) The ISC on Internet Governance shall, at all times, conduct its affairs in an open, transparent and accountable manner, and be responsive to the needs of the public and to technological developments.** In addition to these amendments to the Cybercrimes Bill, the establishment of the Interdepartmental Steering Committee on Internet Governance would also necessitate the amendment and/or rationalisation of an array of other legislation, and

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		regulations and policies published thereunder, that deal with matters related to internet governance. Such amendments are necessary to ensure that the desired coordination is achieved. This may be achieved through a schedule of amendments contained as a schedule to the CCB. The necessary laws may include: 1. ECTA; 2. POPIA; 3. Films and Publications Act; 4. Copyright Act 98 of 1978; 5. Electronic Communications Act 36 of 2005; 6. Intelligence Services Act 65 of 2002; 7. Intelligence Oversight Act 40 of 1994; 8. National Strategic Intelligence Act 39 of 1994; 9. Financial Intelligence Centre Act 38 of 2001 10. Prevention and Combating of Hate Crimes and Hate Speech Bill [2016].
Impact Assessment of the Bill	**MTN**	MTN expressed concern that a regulatory impact assessment has not been conducted to assess the following: • The cost of compliance • The level of expertise available with law enforcement and other government departments to establish cybersecurity hubs and • The privacy rights as conferred to in POPI vis a vis the rights conferred upon law enforcement in accordance with this Bill.
	MMA	As MMA has previously noted in the submissions to the National Assembly, following the establishment of the SEIAS by the Cabinet in February 2007, from 1 October 2015 any Cabinet Memoranda seeking approval for draft policies, bills, or regulations must include a socio-economic impact assessment compiled and approved by the SEIAS Unit.1 The SEIAS, which replaces the Regulatory Impact Assessment, aims to "minimise unintended consequences from policy initiatives, regulations and legislation, including unnecessary costs from implementation and compliance as well as from unanticipated outcomes", and "to anticipate implementation risks and encourage measures to mitigate them"

PROVISION IN QUESTION	NAME OF COMMENTATOR	SUBMISSION/RECOMMENDATION
		In the even that such an impact assessment has been completed, this should be made public without delay, and stakeholders should be permitted the opportunity to make submissions on the impact assessment. The impact assessment is a self-imposed Cabinet obligation and a necessary tool in better understanding internet governance proposals within the state. In the event that an impact assessment has not been completed, further deliberations on the Cybercrimes Bill should be halted until this has been done and all relevant stakeholders have had the opportunity to consider and make submissions thereon.

ANNEXURE B

RECOMMENDED AMENDMENTS TO THE

CYBERCRIMES BILL B6B — 2017

1	**Definitions and Interpretation**	**"article"** means any— *(a)* data; *(b)* computer program; *(c)* computer data storage medium, or *(d)* computer system which— (i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission; (ii) may afford evidence of the commission or suspected commission; or (iii) is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission of— *(aa)* an offence in terms of Part I and Part II of Chapter 2; *(bb)* and other offence in terms of the law of the Republic; or *(cc)* an offence in a foreign State that is substantially similar to an offence contemplated in Part I or Part II of Chapter 2 or another offence recognised in the Republic; **["Companies Act, 2008'' means the Companies Act, 2008 (Act No. 71 of 2008);]** **"Constitution"** means the Constitution of the Republic of South Africa, 1996; **"Electronic Communications Act, 2005"** means the Electronic Communications Act, 2005 (Act No. 36 of 2005); **["electronic communications identity number" means a technical identification label which represents the origin or destination of electronic communications traffic, as a rule clearly identified by a logical or virtual identity number or address assigned to a customer of an electronic communications service provider (such as a telephone number, cellular phone number, email address with or without a corresponding IP address, Web address with or without a corresponding IP address or other subscriber number);]** **"electronic communications network"** means an "electronic communications network" as defined in section 1 of the Electronic Communications Act, 2005, and includes a computer system; **"electronic communication service"** means any service which consists wholly

		or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services as defined in section 1 of the Electronic Communications Act, 2005; **"electronic communications service provider"** means— *(a)* any person who provides an electronic communications service to the public, sections of the public, the State, or the subscribers to such service, under and in accordance with an electronic communications service licence issued to **[such]** that person **[under Chapter 3]** in terms of the Electronic Communications Act, 2005, or who is deemed to be licenced or exempted from being licenced as such in terms of that Act; and *(b)* a person who has lawful authority to control the operation or use of a private electronic communications network used primarily for providing electronic communications services for the owner's own use and which is exempted from being licensed in terms of the Electronic Communications Act, 2005; **["Labour Relations Act, 1995" means the Labour Relations Act, 1995 (Act No. 66 of 1995);]** **"National Commissioner"** means the National Commissioner of the South African Police Service, appointed by the President under section 207(1) of the Constitution **[of the Republic of South Africa, 1996]**; **"National Director of Public Prosecutions"** means the person contemplated in section 197(1)*(a)* of the Constitution **[of the Republic of South Africa, 1996]** and appointed in terms of section 10 of the National Prosecuting Authority Act, 1998; **["National Environmental Management Act, 1998" means the National Environmental Management Act, 1998 (Act No. 107 of 1998);]** **"National Head of the Directorate"** means a person appointed in terms of section 17CA(1) of the South African Police Service Act, 1995 **[(Act No. 68 of 1995]**; **"police official"** means a member of the South African Police Service as defined in section 1 of the South African Police Service Act, 1995 **[(Act No. 68 of 1995])**; **["Prevention and Combating of Corrupt Activities Act, 2004" means the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004);]** **["Protected Disclosures Act, 2000" means the Protected Disclosures Act, 2000 (Act No. 26 of 2002;]**

		"responsible party" means a 'responsible party' as defined in section 1 of the Protection of Personal Information Act, 2013; **"South African Police Service Act, 1995"** means the South African Police Service Act, 1995 (Act No. 68 of 1995); **"South African Reserve Bank"** means the South African Reserve Bank, referred to in section 223 of the Constitution **[of the Republic of South Africa, 1996]**, read with section 2 of the South African Reserve Bank Act, 1989; **"specifically designated police official"** means a police official of the rank of captain or above referred to in section 33 of the South African Police Service Act, 1995 **[(Act No. 68 of 1995)]**, who has been designated in writing by the National Commissioner and the National Head of the Directorate, respectively, to— **[(i)]** *(a)* make oral applications for a search warrant or an amendment of a warrant contemplated in section 30; **[(ii)**] *(b)* issue expedited preservation of data directions contemplated in section 41; or **[(iii)]** *(c)* serve or execute an order from the designated judge as contemplated in section 48(10); (2) For the purposes of section 2, 3(2) or (3), or 7(1) or (2) of this Act, any failure by a responsible party to comply with— *(a)* the conditions for lawful processing of personal information referred to in Chapter 3; *(b)* section 72; or *(c)* the provisions of a code of conduct issued in terms of section 60, of the Protection of Personal Information Act, 2013, must be dealt with in terms of Chapter 10 of that Act.
2	**Unlawful access**	**[(1) Any person who unlawfully and intentionally accesses—** ***(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 accesses—** ***(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; or **(iv) otherwise use the data;** ***(b)*** **a computer program when the person is in a position to—** **(i) alter, modify or delete the computer program;** **(ii) copy or move the computer program to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;** **(iii) cause a computer program to perform any function;** **(iv) obtain its output; or** **(v) otherwise use the computer program;** ***(c)*** **a computer data storage medium when the person is in a position to—** **(i) access data as contemplated in paragraph *(a)* or access a computer program as contemplated in paragraph *(b)*, stored on the computer data storage medium;** **(ii) store data or a computer program on a computer data storage medium; or** **(iii) otherwise use the computer data storage medium; or** ***(d)*** **a computer system when the person is in a position to—** **(i) use any resources of;** **(ii) instruct; or** **(iii) communicate with,** **a computer system.** **(3) For purposes of subsection (1), the actions of a person, to the extent that such actions exceed his or her lawful authority to access data, a computer program, a computer data storage medium or a computer system, must be regarded as unlawful.]** (1) Any person who unlawfully and intentionally performs an act— (a) in respect of a computer system; or (b) a computer data storage medium, which places the person who performed the act or any other person in a position to commit an offence contemplated in subsection (2), section 3(1), 5(1) or 6(1), is guilty of an offence. (2)(*a*) Any person who unlawfully and intentionally accesses a computer system or a computer data storage medium, is guilty of an offence. (*b*) For purposes of paragraph (*a*)— (i) a person accesses a computer data storage medium, if the person— (*aa*) uses data or a computer program stored on a computer data storage medium; or (*bb*) stores data or a computer program on a computer data storage medium; and (ii) a person accesses a computer system, if the person— (*aa*) uses data or a computer program held in a computer system;

		(*bb*) stores data or a computer program on a computer data storage medium forming part of the computer system; or (*cc*) instructs, communicates with, or otherwise uses, the computer system. *(c)* For purposes of paragraph (*b*)— (i) a person uses a computer program, if the person— (*aa*) copies or moves the computer program to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium; (*bb*) cause a computer program to perform any function; or (*cc*) obtain the output of a computer program; and (ii) a person uses data, if the person— (*aa*) copies or moves the data to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium; or (*bb*) obtain the output of data.
3	**Unlawful interception of data**	(2) Any person who unlawfully and intentionally possesses data or the output of data, with the knowledge that such data was intercepted unlawfully as contemplated in subsection (1), is guilty of an offence. (3) Any person who is found in possession of data or the output of data, in regard to which there is a reasonable suspicion that such data was intercepted unlawfully as contemplated in subsection (1) and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.
4	**Unlawful acts in respect of software or hardware tool**	(1) Any person who unlawfully and intentionally— *(a)* uses; or *(b)* possesses, any software or hardware tool for purposes of contravening the provisions of section 2(1) or (2), 3(1), 5(1), 6(1) or 7(1)*(a)* or *(d)*, is guilty of an offence. (2) For purposes of this section **"software or hardware tool"** means any electronic, mechanical or other instrument, device, equipment, apparatus or a substantial component thereof or a computer program, which is designed or adapted primarily for the purposes to— *(a)* access as contemplated in section 2(1) or (2); *(b)* intercept data as contemplated in section 3(1); *(c)* interfere with data or a computer program as contemplated in section 5(1); *(d)* interfere with a computer data storage medium or a computer system as contemplated in section 6(1); or *(e)* acquire, make available or use a password, access code or similar data or devices as defined in section 7(3).
5	**Unlawful interference**	(2) For purposes of this section, **"interferes with data or a computer program"** means to permanently or temporarily—

	with data or computer program	*(a)* delete data or a computer program; *(b)* alter data or a computer program; *(c)* render vulnerable, damage or deteriorate data or a computer program; *(d)* render data or a computer program meaningless, useless or ineffective; *(e)* obstruct, interrupt or interfere with the lawful use of, data or a computer program; or *(f)* deny access to data or a computer program, held in a computer system or a computer data storage medium.
6	**Unlawful interference with a computer data storage medium or computer system**	(2) For purposes of this section **"interferes with a computer data storage medium or a computer system"** means to permanently or temporarily— *(a)* alter any resource **[of]**; or *(b)* interrupt or impair— (i) the functioning **[of]**; (ii) the confidentiality **[of]**; (iii) the integrity **[of]**; or (iv) the availability **[of]**, of a computer data storage medium or a computer system.
7	**Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device**	(1) Any person who unlawfully and intentionally— *(a)* acquires; *(b)* possesses; *(c)* provides to another person; or *(d)* uses, a password, an access code or similar data or device for purposes of contravening the provisions of section 2(1) or (2), 3(1), 5(1), 6(1), 8 or 9(1), is guilty of an offence. (2) Any person who is found in possession of a password, an access code or similar data or device in regard to which there is a reasonable suspicion that such password, access code or similar data or device— *(a)* was acquired; *(b)* is possessed; *(c)* is to be provided to another person; or *(d)* was used or may be used, for purposes of contravening the provisions of section 2(1) or (2), 3(1), 5(1), 6(1), 8 or 9(1), and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence. (3) For purposes of this section **"password, access code or similar data or device" [means without limitation]** includes— *(a)* a secret code or pin; *(b)* an image; *(c)* a security token; *(d)* an access card;

		(e) any device; *(f)* biometric data; or *(g)* a word or a string of characters or numbers, used for**[—** **(i) financial transactions; or** **(ii) user authentication in order to access or use data, a computer program, a computer data storage medium or a computer system]** financial transactions or user-authentication in order to access or use data, a computer program, a computer data storage medium or a computer system.
8	**Cyber fraud**	Any person who unlawfully and with the intention to defraud makes a misrepresentation— *(a)* by means of data or a computer program; or *(b)* through any interference with data or a computer program as contemplated in **[subsection]** section 5(2)(*a*), (*b*) or (*e*) or interference with a computer data storage medium or a computer system as contemplated in section 6(2)(*a*), which**[—** **(i) causes actual prejudice; or** **(ii) is potentially prejudicial,]** causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud.
10	**Cyber extortion**	Any person who unlawfully and intentionally commits or threatens to commit any offence as**[—** ***(a)* threatens to commit any offence; or** ***(b)* commits any offence,]** contemplated in sections 3(1), 5(1), 6(1) or 7(1)*(a)* or *(d)*, for the purpose of— *(a)* obtaining any advantage from another person; or *(b)* compelling another person to perform or to abstain from performing any act, is guilty of the offence of cyber extortion.
11	**Aggravated Offences**	(1) *(a)* Any person who commits an offence referred to in— (i) section 3(1), 5(1) or 6(1), in respect of; or (ii) section 7(1), in so far as the passwords, access codes or similar data and devices relate to, a restricted computer system, and who knows or ought reasonably to have known or suspected that it is a restricted computer system, is guilty of an aggravated offence. *(b)* For purposes of paragraph *(a)* **"a restricted computer system"** means any data, computer program, computer data storage medium or computer system **[under the control of, or exclusively used by]**— **[(i) any financial institution; or** **(ii) an organ of state as set out in section 239 of the Constitution of the Republic of South Africa, 1996, including a court.]**

		(i) under the control of, or exclusively used by— *(aa)* a financial institution; or *(bb)* an organ of state as set out in section 239 of the Constitution, including a court; and (ii) which is protected by security measures against unauthorised access or use. (2) Any person who commits an offence referred to in section 5(1), 6(1) or 10, and who knows or ought reasonably to have known or suspected that the offence in question will— **[*(a)* endanger the life, or violate the physical integrity or physical freedom of, or cause bodily injury to, any person, or any number of persons;** ***(b)* cause serious risk to the health or safety of the public or any segment of the public;** ***(c)* cause the destruction of or substantial damage to any property;** ***(d)* cause a serious interference with, or serious disruption of an essential service, facility or system, or the delivery of any essential service;** ***(e)* cause any major economic loss;** ***(f)* create a serious public emergency situation; or** ***(g)* prejudice the security, the defence, law enforcement or international relations of the Republic,]** *(a)* endanger the life or cause serious bodily injury to, or the death of, any person, or any number or group of persons; *(b)* cause serious risk to the health or safety of the public or any segment of the public; or *(c)* create a serious public emergency situation, is guilty of an aggravated offence. (3) The Director of Public Prosecutions having jurisdiction must authorise in writing a prosecution in terms of subsections (1) or (2)**[must be authorised in writing by the Director of Public Prosecutions having jurisdiction]**.
13	**Definitions**	In **[this]** Part II of this Act, unless the context indicates otherwise— **"damage to property"** means damage to any corporeal or incorporeal property; **"discloses"**, in respect of a data message referred to in section 14, 15 and 16, means to— *(a)* send the data message to a person who is the intended recipient of the electronic communication or any other person; *(b)* store the data message on an electronic communications network, where the data message can be viewed, copied or downloaded; or *(c)* send or otherwise make available to a person, a link to the data message that has been stored on an electronic communication network, where the data message can be viewed, copied or downloaded;

14	**Data message which incites damage to property or violence**	Any person who **[unlawfully makes available, broadcasts or distributes]** discloses, by means of **[a computer system]** an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite— *(a)* the causing of any damage to property belonging to; or *(b)* violence against, a person or a group of persons, is guilty of an offence.
15	**Data message which threatens persons with damage to property or violence**	**[(1)]** A person commits an offence if **[he or she]** they, by means of an electronic communications service, unlawfully and intentionally **[makes available, broadcasts or distributes, by means of a computer system,]** discloses a data message, which— **[*(a)* threatens a person with—** **(i) damage to property belonging to, or violence against that person; or** **(ii) damage to property belonging to, or violence against a related person; or** ***(b)* threatens—** **(i) a group of persons;** **(ii) any person forming part of that group of persons; or** **(iii) any person associated with that group or persons,** **with damage to property belonging to, or violence against—** **(aa) that group of persons;** **(bb) any person who forms part of that group of persons; or** **(cc) any person who is associated with that group of persons,]** *(a)* threatens a person with— (i) damage to property belong to that person or a related person; or (ii) violence against that person or a related person; or *(b)* threatens a group of persons or any person forming part of, or associated with, that groups of persons with— (i) damage to property belonging to that group of persons or any person forming part of, or associated with, that groups of persons; or (ii) violence against group of persons or any person forming part of, or associated with, that groups of persons, and a reasonable person in possession of the same information, **[and]** with due regard to all the circumstances, would **[regard]** perceive the data message, either by itself or in conjunction with any other data message or information, as a threat of damage to property or violence to a person or category of persons contemplated in paragraph *(a)* or *(b)*, respectively.
16	**[Distribution] Disclosure of data message of intimate image**	(1) Any person ("A") who unlawfully and intentionally discloses, **[makes available, broadcasts or distributes, by means of a computer system]** by means of **[a computer system]** an electronic communications service, a data message of an intimate image of a person ("B"), without the consent of B, is guilty of an offence.

		(2) For purposes of subsection (1)— *(a)* **''B''** means— (i) the person who can be identified as being displayed in the data message; (ii) any person who is described as being displayed in the data message, irrespective of the fact that **[he or she]** the person cannot be identified as being displayed in the data message; or (iii) any person who can be identified from other information as being displayed in the data message; and *(b)* **''intimate image''** means a depiction of a person— (i) real or simulated and made by any means in which— *(aa)* B is nude, or **[his or her]** the genital organs or anal region of B is displayed, or if B is a female person, transgender person or intersex person, their breasts, are displayed; or *(bb)* the covered genital or anal region of B, or if B is a female person, transgender person or intersex person, their covered breasts, are displayed **[in a manner that violates or offends the sexual integrity or dignity of B]**; and (ii) in respect of which B so displayed retains a reasonable expectation of privacy at the time that the data message was made in a manner that— *(aa)* violates or offends the sexual integrity or dignity of B; or *(bb)* amounts to sexual exploitation.
18	**Competent Verdicts**	(2) If the evidence on a charge of a contravention of section 3(1), does not prove the offence or a contravention of section 17 in respect of that offence, but proves a contravention of— *(a)* **[a contravention of]** section 2(1) or (2); *(b)* **[a contravention of]** section 3(2) or (3); or *(c)* **[a contravention of]** section 4(1) in so far as it relates to the use or possession of a software or hardware tool for purposes of contravening section 3(1), the accused may be found guilty of the offence so proved. (3) If the evidence on a charge of a contravention of section 5(1), does not prove the offence or a contravention of section 17 in respect of that offence, but proves— *(a)* a contravention of section 2(1) or (2); *(b)* a contravention of section 4(1) in so far as it relates to the use or possession of a software or hardware tool for purposes of contravening section 5(1); or *(c)* the offence of malicious injury to property, the accused may be found guilty of the offence so proved. (4) If the evidence on a charge of a contravention of section 6(1), does not prove the offence or a contravention of section 17 in respect of that offence, but proves—

		(a) a contravention of section 2(1) or (2); *(b)* a contravention of section 4(1) in so far as it relates to the use or possession of a software or hardware tool for purposes of contravening section 6(1); or *(c)* the offence of malicious injury to property, the accused may be found guilty of the offence so proved. (5) *(a)* If the evidence on a charge of a contravention of section 7(1)*(a)* or *(d)* does not prove the offence or a contravention of section 17 in respect of that offence, but proves a contravention of— (i) **[a contravention of]** section 2(1) or (2); (ii) **[a contravention of]** section 7(1)*(b)* or *(c)* or (2); or (iii) **[a contravention of]** section 4(1) in so far as it relates to the use or possession of a software or hardware tool to acquire or use a password, access code or similar data or device, the accused may be found guilty of the offence so proved. *(b)* If the evidence on a charge of a contravention of section 7(1)*(b)* or *(c)* does not prove the offence or a contravention of section 17 in respect of that offence, but proves a charge of a contravention of section 7(2), the accused may be found guilty of the offence so proved. (6) If the evidence on a charge of a contravention of section 8, does not prove the offence or a contravention of section 17 in respect of the offence, but proves — *(a)* a contravention of section 2(1) or (2); *(b)* a contravention of section 4(1), in so far as it relates to the use or possession of a software or hardware tool for the purposes of— (i) interfering with data or a computer program as contemplated in section 5(1); or (ii) interfering with a computer data storage medium or a computer system as contemplated in section 6(1); *(c)* a contravention of section 7(1) or (2), in so far as the password, access code or similar data or device was acquired, possessed, provided to another person or used for purposes of contravening the provisions of section 8; *(d)* a contravention of section 9(1) or (2); *(e)* the common law offence of fraud or attempt to commit that offence; *(f)* the common law offence of forgery or uttering or attempt to commit that offence; or *(g)* the common law offence of theft or attempt to commit that offence, the accused may be found guilty of the offence so proved. (8) If an accused is charged with a contravention of section 11(1), and the evidence on the charge does not prove a contravention of section 11(1) or a contravention of section 17 in respect of that offence, but a proves a contravention of—

		(a) section 2(1) or (2); *(b)* section 3(1) or any competent verdict provided for in subsection (2); *(c)* section 5(1) or any competent verdict provided for in subsection (3); *(d)* section 6(1) or any competent verdict provided for in subsection (4); or *(e)* section 7(1) or any competent verdict provided for in subsection (5), the accused may be found guilty of the offence so proved. (9) If an accused is charged with a contravention of section 11(2) or a contravention of section 17 in respect of that offence, and the evidence on the charge does not prove a contravention of section 11(2), but **[a]** proves a contravention of— *(a)* section 2(1) or (2); *(b)* section 5(1) or any competent verdict provided for in subsection (3); or *(c)* section 6(1) or any competent verdict provided for in subsection (4), the accused may be found guilty of the offence so proved.
19	**Sentencing**	(1) Any person who contravenes the provisions of section 2(1) or (2), 3(3) or 7(2) is liable on conviction to a fine or to imprisonment for a period not exceeding five years or to both a fine and such imprisonment. (6) *(a)* If a person is convicted of any offence provided for in section 2(1) or (2), 3(1), 5(1), 6(1), 7(1), 8, 9(1) or (2), 10 or 11(1) or (2), a court **[which imposes]** imposing any sentence in terms of those sections **[where]** must, unless substantial and compelling circumstances justify the imposition of another sentence, impose a period of direct imprisonment, with or without a fine, if the offence was committed— (i) by the person; or (ii) with the collusion or assistance of another person, who as part of **[his or her]** their duties, functions or lawful authority **[was]** were in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system belonging to another person in respect of which the offence in question was committed**[, must, unless substantial and compelling circumstances justifying the imposition of another sentence impose, with or without a fine, a period of direct imprisonment which]**. *(b)* A sentence imposed in terms of *(a)* may not be suspended as contemplated in section 297(4) of the Criminal Procedure Act, 1977.
20	**Order to protect complainant pending finalisation of criminal proceedings**	(1) A complainant (hereinafter referred to as the applicant) who lays a charge with the South African Police Service that an offence contemplated in section 14, 15 or 16 has allegedly been committed against **[him or her]** them, may on an *ex parte* basis in the prescribed form and manner, apply to a magistrate's court for an order pending the finalisation of the criminal proceedings to— *(a)* prohibit any person **[from further making available, broadcasting or distributing the data message contemplated in section 14, 15 or 16 which relates to the charge]** to disclose or further disclose the data

		message which relates to the charge; or *(b)* order an electronic communications service provider **[or person in control of a computer system to]** whose electronic communications service is used to host or disclose the data message which relates to the charge to remove or disable access to the data message **[in question]**. (3) If the court is satisfied that there is— *(a)* *prima facie* evidence that **[the data message in question constitutes an offence as contemplated]** an offence referred to in section 14, 15 or 16, has allegedly been committed against the applicant; *(b)* reasonable grounds to believe that a person referred to in subsection (1)*(a)* disclosed the data message in question; or *(c)* reasonable grounds to believe that the electronic communications service of the electronic communications service provider is used to host or was or is used to disclose the data message in question, the court may, subject to such conditions as the court may deem fit, issue the order referred to in subsection (1), in the prescribed form. (4) The order, referred to in subsection (3), must be served on the person referred to in subsection (1)*(a)* or electronic communications service provider **[or person]** referred to in subsection (1)*(b)* in the prescribed **[form and]**: Provided, that if the court is satisfied that the order cannot be served in the prescribed **[form and]** manner, the court may make an order allowing service to be effected in the form or manner specified in that order. (5) An order referred to in subsection **[(1)]**(3) is of force and effect from the time it is issued by the court and the existence thereof has been brought to the attention of the person referred to in subsection (1)(*a*) or electronic communications service provider referred to in subsection (1)(*b*). (6) A person referred to in subsection (1)(*a*), other than the person who is accused of having committed the offence in question, or an electronic communications service provider **[or person,]** referred to in subsection (1)(*b*), may, within **[30]**14 days after the order has been served on **[him, her or it]** them in terms of subsection (4), or within such further period as the court may allow, upon notice to the magistrate's court concerned, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection **[(1)]**(3). (7)*(a)* The court must as soon as reasonably possible consider an application submitted to it in terms of subsection (6) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which **[shall]** must form part of the record of the proceedings. *(b)* The court may if good cause is shown for the variation or setting aside of the protection order, issue an order to this effect.

		(8) The court may, for purposes of subsection (2) and (7), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case. (9) Any person referred to in subsection (1)*(a)* or an electronic communications service provider, referred to in subsection (1)*(b)*, **[who]** that fails to comply with an order referred to in subsection **[(5)]**(3), or any variations thereof, is guilty of an offence. (12) For purposes of this section and sections 21 and 22 **"to host a data message"** means to store the data message on an electronic communications network that is used to provide an electronic communications service, where it can be viewed, copied and downloaded.
21	**Electronic communications service provider [or person in control of computer system to furnish particular to court**	(1) If an application for a protection order is made in terms of section 20(1) and the court is satisfied in terms of section 20(3) that a protection order must be issued and the **[identity or address of the person]** particulars of the person referred to in section 20(1)*(a)* who discloses the data message or the electronic communications service provider, referred to in section 20(1)*(b)*, whose service is used to host or was or is used to disclose the data message **[who made available, broadcasted or distributed the data message in question]** is not known, the court may— *(a)* adjourn the proceedings to any time and date on the terms and conditions which the court deems appropriate; and *(b)* issue a direction in the prescribed form, directing an electronic communications service provider, that is believed to be able to furnish such particulars, **[or person in control of a computer system]** to furnish the court in the prescribed manner by means of an affidavit in the prescribed form with— (i) the electronic communications identity number from where the data message originated; (ii) the name, surname, identity number and address of the person to whom the electronic communications identity number has been assigned; (iii) any information which indicates that the data message was or was not sent from the electronic communications identity number of the person to the electronic communications identity number of the complainant; and (iv) any **[other]** information that is available to an electronic communications service provider that may be of assistance to the court to identify the person referred to in section 20(1)*(a)* or the electronic service provider referred to in section 20(1)*(b)*, **[or a person in control of a computer system which may be of assistance to the court to identify the person who made available,**

		broadcasted or distributed the data message in question or the electronic communications service provider or person in control of a computer system] which provides a service to **[the]** that person **[who made available, broadcasted or distributed the data message]**; (v) any information that is available to an electronic communications service provider which— (*aa*) confirms whether or not its electronic communications service is used to host or was or is used to disclose the data message in question; or (*bb*) may be of assistance to the court to identify the electronic communications service provider whose service is used to host or was or is used to disclose the data message in question; and (vi) an assessment whether or not the electronic communications service provider is in a position— (*aa*) to remove the data message or a link to the data message; or (*bb*) to disable access to such data message or a link to such data message. (2) If the court issues a direction in terms of subsection (1) the court must direct that the direction be served on the electronic communications service provider **[or person in control of a computer system]** in the prescribed manner; Provided, that if the court is satisfied that the direction cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form and manner specified in that order. (3)*(a)* The information referred to in subsection (1)*(b)***[(i), (ii), (iii) and (iv)]** must be provided to the court within five ordinary court days from the time that the direction is served on an electronic communications service provider **[or person in control of a computer system]**. *(b)* An electronic communications service provider **[or person in control of a computer system]** on which a direction is served, may in the prescribed manner by means of an affidavit in the prescribed form apply to the court for— (i) an extension of the period of five ordinary court days referred to in paragraph *(a)* for a further period of five ordinary court days on the grounds that the information cannot be provided timeously; or (ii) the cancellation of the direction on the grounds that— *(aa)* it does not provide an electronic communications service to **[either the respondent or complainant or related person]** the applicant or the person referred to in section 20(1)*(a)*; **[or]** *(bb)* the requested information is not available in the records of the electronic communications service provider **[or person in control of a computer system.]**; or *(cc)* its service is not used to host or was or is not used to disclose the data message in question.

		(4) After receipt of an application in terms of subsection (3)*(b)*, the court— *(a)* must consider the application; *(b)* may, in the prescribed manner, request such additional evidence by way of affidavit from the electronic communications service provider **[or the person in control of a computer system]** as it deems fit; *(c)* must give a decision in respect thereof; and *(d)* must inform the electronic communications service provider **[or the person in control of a computer system]** in the prescribed form and in the prescribed manner of the outcome of the application. (5)*(a)* The court may, on receipt of an affidavit from an electronic communications service provider **[or person in control of a computer system]** which contains the information referred to in subsection (1)*(b)*, consider the issuing of a protection order in terms of section 20(3) against the person or electronic communications service provider **[who made available, broadcasted or distributed the data message contemplated in section 14, 15 or 16]** on the date to which the proceedings have been adjourned. *(b)* Any information furnished to the court in terms of subsection (1)*(b)* forms part of the evidence that a court may consider in terms of section 20(3). (6) The Cabinet member responsible for the administration of justice may, by notice in the *Gazette*, prescribe reasonable tariffs of compensation payable to electronic communications service providers **[or person in control of a computer system]** for providing the information referred to in subsection (1)*(b)*. (7) Any electronic communications service provider or employee of an electronic communications service provider **[or person in control of a computer system]** who— *(a)* fails to furnish the required information within five ordinary court days from the time that the direction is served on such electronic communications service provider **[or person in control of a computer system]** to a court in terms of subsection (3)*(a)* or such extended period allowed by the court in terms of subsection (3)*(b)*; or *(b)* makes a false statement in an affidavit referred to in subsection (1)*(b)* or (3)*(b)* in a material respect, is guilty of an offence. (8) For purposes of this section "**electronic communications identity number**" means a technical identification label that represents the origin or destination of electronic communications traffic.
22	**Orders on finalisation of criminal proceedings**	(1) Whenever a person is— *(a)* convicted of an offence in terms of section 14, 15 or 16; or *(b)* acquitted of an offence in terms of section 14, 15 or 16, but evidence proves that the person engaged in, or attempted to engage in,

		harassment as contemplated in the Protection from Harassment Act, 2011, the trial court may, after holding an enquiry, issue a protection order contemplated in section 9(4) of the Protection from Harassment Act, 2011, against the person, whereafter the provisions of that Act shall apply with the necessary changes as required by the context. (2) The trial court **[must, on convicting]** which convicts a person **[for the commission]** of an offence contemplated in section 14, 15 or 16, must order— *(a)* that person to refrain from further making available, broadcasting or distributing the data message contemplated in section 14, 15 or 16 which relates to the charge on which **[he or she]** that person is convicted; *(b)* that person or any other person to destroy the data message in question, any copy of the data message or any output of the data message and to submit an affidavit in the prescribed form to the prosecutor identified in the order that the data message has been so destroyed; or *(c)* an electronic communications service provider **[or person in control of a computer system]** to remove or disable access to the data message in question. (3) The order referred to in subsection (2)*(b)*, in so far as it relates to a person other than the **[accused]** person who has been convicted of the offence, and (2)*(c)*, must be in the prescribed form and must be served on the electronic communications service provider **[or person in control of a computer system]** in the prescribed manner: Provided, that if the trial court is satisfied that the order cannot be served in the prescribed form and manner, the court may make an order allowing service to be effected in the form and manner specified in that order. (4) Any person contemplated in subsection (2)*(a)* or *(b)* or electronic communications service provider **[or person in control of a computer system]** contemplated in subsection (2)*(c)* **[who]** that fails to comply with an order referred to in subsection (2) is guilty of an offence. (5) An electronic communications service provider that is ordered to remove or disable access to the data message, may, within 14 days after the order has been served on it, in terms of subsection (3), upon notice to the trial court concerned, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection (2)*(c)*. (6)*(a)* The trial court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (5) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings. *(b)* The trial court may if good cause has been shown for the variation or setting aside of the order, issue an order to this effect.

		(7) The court may, for purposes of subsection (6)*(a)*, in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case. (8) Any person who is subpoenaed in terms of subsection (7) to attend proceedings and who fails to— *(a)* attend or to remain in attendance; *(b)* appear at the place and on the date and at the time to which the proceedings in question may be adjourned; *(c)* remain in attendance at those proceedings as so adjourned; or *(d)* produce any book, document or object specified in the subpoena, is guilty of an offence. **[(5)]**(9) For purposes of this section **"trial court"** means— *(a)* a magistrate's court established under section 2(1)*(f)*(i) of the Magistrates' Courts Act, 1944; *(b)* a court for a regional division established under section 2(1)*(g)*(i) of the Magistrates' Courts Act, 1944; or *(c)* a High Court referred to in section 6(1) of the Superior Courts Act, 2013. **[(6)]**(10) Whenever a person is convicted of an offence in terms of section 14, 15 or 16, the trial court must issue an order that the person must reimburse all expenses reasonably incurred by— *(a)* a complainant as a result of any direction issued in terms of section 21(1)*(b)*; or *(b)* an electronic communications service provider **[or person in control of a computer system]** to remove or disable access to the data message in question, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context, to such order.
23	**Penalties**	Any person or electronic communications service provider **[who contravenes the provisions of]** that is convicted of an offence referred in section 20(9) or (10), 21(7) or 22(4) or (8) is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both a fine and such imprisonment.
24	**Jurisdiction**	(1) A court in the Republic **[trying an offence]** has jurisdiction **[where]** to try any offence referred to in Part I or Part II of Chapter 2, if— *(a)* **[an offence in terms of Part I or Part II of Chapter 2 was committed— (i)]** the accused was arrested in the territory of the Republic**[; or (ii)]** on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic **[at the time the offence was committed]**; *(b)* **[an offence in terms of Part I or Part II of Chapter 2 was committed,**

		in the Republic, or outside the Republic, against a person who] the person to be charged is— (i) is citizen of the Republic or ordinarily resident in the Republic; (ii) a company, incorporated or registered as such under any law, in the Republic; or (iii) any body of persons, corporate or unincorporated, in the Republic; *(c)* an offence **[in terms of Part I of Chapter 2]** was committed— (i) in the territory of the Republic**;** or **[outside the Republic, against a person who is—** **(i) a company, incorporated or registered as such under any law, in the Republic; or** **(ii) any body of persons, corporate or unincorporated, in the Republic;]** (ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, on an aircraft registered or required to be registered in the Republic at the time that the offence was committed; **[*(d)* an offence in terms of Part I of Chapter 2 was committed, in the Republic, or outside the Republic, against—** **(i) a restricted computer system contemplated in section 11(1)*(b)*; or** **(ii) a government facility of the Republic abroad, including an embassy or other diplomatic or consular premises, or any other property of the Republic; or]** *(d)* any act in preparation of an offence **[in terms of Part I or Part II of Chapter 2,]** or any action necessary to commit the offence or any part of the offence took place— (i) in the territory of the Republic; or (ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time when the act, action or part of the offence **[was committed]** took place; *(e)* the offence affects any person, a restricted computer system contemplated in section 11(1)(*b*), a public body or any business, in the Republic; (*f*) the offence was committed outside the Republic against— (i) any person who is citizen of the Republic or ordinarily resident in the Republ*i*c; (ii) a restricted computer system contemplated in section 11(1)(*b*); (iii) a company, incorporated or registered as such under any law, in the Republic; (iv) any body of persons, corporate or unincorporated, in the Republic; or (v) a government facility of the Republic, including an embassy or other diplomatic or consular premises, or any other property of the Republic; or (*g*) the evidence reveals any other basis recognised by law in terms of which the court may assert jurisdiction to try the offence. (2) **[if the]** Any act alleged to constitute an offence in terms of Part I or Part

		II of Chapter 2 and which was committed outside the Republic by a person other than a person contemplated in subsection (1), must, **[a court of the Republic,]** regardless of whether or not the act constitutes an offence at the place of its commission, **[has jurisdiction in respect of that offence if the person to be charged]** be deemed to have been committed in the Republic if — *(a)* that person is extradited to the Republic; or **[is a citizen of the Republic or ordinarily resident in the Republic]**; or *(b)* that person— (i) is found to be in Republic; and (ii) is for one or other reason not extradited by the Republic or if there is no application to extradite the person **[arrested in the territory of the Republic, or in its territorial waters or on board a ship or aircraft registered or required to be registered in the Republic at the time the offence was committed;** ***(c)* is a company, incorporated or registered as such under any law, in the Republic; or** ***(d)* any body of persons, corporate or unincorporated, in the Republic]**. (3) Where a person is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offence, the offence is deemed to have been committed not only at the place where the act was committed, but also at every place where the person so acted. **[(3)]**(4)*(a)* A prosecution of **[Any act alleged to constitute]** an offence **[in terms]** referred to in Part I or Part II of Chapter 2**, [and]** which was committed outside the Republic **[by a person, other than a person contemplated in subsection (2), is, regardless of whether or not the act constitutes an offence or not at the place of its commission, deemed also to have been committed in the Republic if that—** ***(a)* person is found to be in South Africa; and** ***(b)* person is for one or other reason not extradited to, or by South Africa, or if there is no application to extradite that person—** (i) may only be instituted against a person with the written permission of the National Director of Public Prosecutions; and (ii) must commence before a court designated by the National Director of Public Prosecutions. *(b)* The accused must be served with a copy of the written permission and designation and the original thereof must be handed in at the court in which the proceedings are to commence. **[(4) Where a person is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offence, the offence is deemed to have been committed not only at the place where the**

		act was committed, but also at every place where the person acted.] **[(5) *(a)* A prosecution in terms of subsections (2) and (3)—** **(i) may only be instituted against a person with the written permission of the National Director of Public Prosecutions; and** **(ii) must commence before a court designated by the National Director of Public Prosecutions.** ***(b)* A copy of the written permission and designation must be served on the accused** **and the original thereof must be handed in at the court in which the proceedings are to commence.]** **[(6)]**(5) The National Commissioner and the National Head of the Directorate, **[respectively,]** in consultation with the National Director of Public Prosecutions must issue directives, with which all police officials must comply in the execution of their functions in terms of this Act regarding the investigation of offences that was committed outside the Republic.
25	**Definitions**	"**access**" includes without limitation to make use of— (a) **[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 thereto; and (b) data and a computer program held in a computer data storage medium or a computer system, to the extent necessary to search for and seize an article.
26	**Standard Operating Procedures**	(1) The Cabinet member responsible for policing, in consultation with the National Commissioner, the National Head of the Directorate, the National Director of Public Prosecutions and the Cabinet member responsible for the administration of justice must, after following a process of public consultation, within **[six]** 12 months of the commencement of this Chapter, issue Standard Operating Procedures which must be observed by— *(a)* the South African Police Service; or *(b)* any other person or agency who or which is authorised in terms of the provision of any other law, **[to investigate]**in the investigation of any offence in terms of any law, in the investigation of any offence or suspected offence in terms of Part I or Part II of Chapter 2 or any other offence or suspected offence which may be committed by means of or facilitated by the use of an article.
29	**Article to be searched for, accessed or seized under search warrant**	(1) Subject to the provisions of sections 31, 32, 33 and 40(1) and (2) of this Act, section 4(3) of the Customs and Excise Act, 1964, sections 69(2)*(b)* and 71 of the Tax Administration Act, 2011, and section 21*(e)* and *(f)* of the Customs Control Act, 2014, an article can only be searched for, accessed or seized by virtue of a search warrant issued— *(a)* by a magistrate or judge of the High Court, on written application by a

		police official, if it appears to the magistrate or judge, from information on oath or by way of affirmation, as set out in the application, that there are reasonable grounds for believing that an article— (i) is within **[his or her]** their area of jurisdiction; or (ii) is being used or is involved or has been used or was involved in the commission of an offence— *(aa)* within **[his or her]** their area of jurisdiction; or *(bb)* within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved or has been used or was involved in the commission of an offence; or *(b)* by a magistrate or judge of the High Court presiding at criminal proceedings, if it appears to such magistrate or judge that an article is required in evidence at such proceedings. (2) A search warrant issued under subsection (1) must require a police official identified in the warrant to search for, access and seize the article in question and, to that end, must authorise the police official to— *(a)* search any person identified in the warrant; *(b)* enter and search any container, premises, vehicle, facility, ship or aircraft identified in the warrant; *(c)* 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; *(d)* 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— (i) is nearby; (ii) uses; or (iii) is in possession **[of]** or in direct control of, any data, computer program, computer data storage medium or computer system identified in the warrant to the extent set out in the warrant; *(e)* search for any article identified in the warrant to the extent set out in the warrant; *(f)* access an article identified in the warrant to the extent set out in the warrant; *(g)* seize an article identified in the warrant to the extent set out in the warrant; or *(h)* use or obtain and use any instrument, device, equipment, password, decryption key, data, computer program, computer data storage medium or computer system or other information that is believed, on reasonable grounds, to be necessary to search for, access or seize an article identified in the warrant to the extent set out in the warrant.
30	**Oral application for**	(4) A warrant or any amendment to a warrant may only be issued under subsection (3)—

	search warrant or amendment of warrant	*(a)* if the magistrate or judge of the High Court concerned is satisfied, on the facts alleged in the oral application concerned, that— (i) there are reasonable grounds to believe that a warrant or any amendment to a warrant applied for could be issued; (ii) a warrant or an amendment to a warrant is necessary immediately in order to search for, access or seize an article— *(aa)* within **[his or her]** their area of jurisdiction; or *(bb)* within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved in the commission of an offence; and (iii) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of a warrant or to amend a warrant; and *(b)* on condition that the police official concerned must submit a written application to the magistrate or judge of the High Court concerned within 48 hours after the issuing of the warrant or amended warrant under subsection (3). (6) A magistrate or judge of the High Court who has issued a warrant or amended a warrant under subsection (3) or, if **[he or she is not available]** unavailable, any other magistrate or judge of the High Court must, upon receipt of a written application **[submitted to him or her]** in terms of subsection (4)*(b)*, reconsider that application whereupon **[he or she]** they may confirm, amend or cancel that warrant. (7) A magistrate or judge of the High Court contemplated in subsection (6), who amends or cancels the warrant, must make an order **[as he or she]** they **[deems]** deem fit on how any article which is affected by **[his or her]** their decision is to be dealt with.
32	**Search for, access to, or seizure of article involved in the commission of an offence without search warrant**	(1) A police official may without a search warrant referred to in section 29(1)*(a)* search any person, container, premises, vehicle, facility, ship or aircraft for the purposes of performing the powers referred to in paragraphs *(a)* and *(b)* of the definition of "seize" in respect of a computer data storage medium or any part of a computer system referred to in paragraph *(c)* or *(d)* of the definition of "article", if the police official on reasonable grounds believes— *(a)* that a search warrant will be issued to **[him or her]** them under section 29(1)*(a)* if **[he or she applies]** they apply for such warrant; and *(b)* that the delay in obtaining such warrant would defeat the object of the search and seizure. (2) A police official may only access or perform the powers referred to in paragraphs *(c)* or *(d)* of the definition of "seize", in respect of the computer data storage medium or a computer system referred to in subsection (1), in accordance with a search warrant issued in terms of section 29(1)*(a)*: Provided

		that a police official may, if they on reasonable grounds believe— *(a)* that a search warrant will be issued to them under section 29(1)*(a)* if they apply for such warrant; and *(b)* it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant, access and perform the powers referred to in paragraph *(c)* or *(d)* of the definition of "seize" without a search warrant.
33	**Search for, access to and seizure of article on arrest of person**	(1) A police official may without a warrant, as contemplated in section 40 of the Criminal Procedure Act, 1977, arrest any person— *(a)* who commits any offence in terms of Part I or Part II of Chapter 2 in **[his or her]** their presence; *(b)* whom **[he or she]** they reasonably **[suspects]** suspect of having committed any offence in terms of Part I and part II of Chapter 2; or *(c)* who is concerned with or against whom a reasonable complaint has been made or credible information has been received or a reasonable suspicion exists that **[he or she has]** they have been concerned with an offence— (i) similar to those contemplated in Part I or Part II of Chapter 2; or (ii) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated by the use of an article, in a foreign State, and for which **[he or she is]** they are, under any law relating to extradition or fugitive offenders, liable to be arrested or detained in custody in the Republic. (2) On the arrest of a person contemplated in subsection (1) or in terms of section 40 or 43 of the Criminal Procedure Act, 1977, a police official may search for and perform the powers referred to in paragraphs *(a)* and *(b)* of the definition of "seize"' in respect of a computer data storage medium or any part of a computer system referred to in paragraph *(c)* or *(d)* of the definition of "article", which is found in the possession of or in the custody or under the control of the person. (3) A police official may only access or perform the powers referred to in paragraphs *(c)* or *(d)* of the definition of "seize", in respect of a computer data storage medium or a computer system referred to in subsection (2), in accordance with a search warrant issued in terms of section 29(1)*(a)*: Provided that a police official may, if they on reasonable grounds believe— *(a)* that a search warrant will be issued to them under section 29(1)*(a)*, if they apply for such warrant; and *(b)* it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant, access and perform the powers referred to in paragraph *(c)* and *(d)* of the definition of "seize" without a search warrant.

35	**Obstructing or hindering police official or investigator and authority to overcome resistance**	(1) Any person who unlawfully and intentionally obstructs or hinders a police official or an investigator in the exercise of **[his or her]** their powers or the performance of **[his or her]** their duties or functions in terms of this Chapter or who refuses or fails to comply with a search warrant issued in terms of section 29(1), is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a find and such imprisonment. (2)*(a)* A police official who may lawfully execute any power conferred upon him or her in terms of section 29(2), may use such force as may be— (i) reasonably necessary; and (ii) proportional to all the circumstances, relating to the execution of such powers. *(b)* No police official may enter upon or search any premises, vehicle, facility, ship or aircraft unless **[he or she has]** they have audibly demanded admission to the premises, vehicle, facility, ship or aircraft and **[has]** have notified the purpose of **[his or her]** their entry. *(c)* The provisions of paragraph *(b)* do not apply where the police official is, on reasonable grounds, of the opinion that an article which is the subject of the search may be destroyed, disposed of or tampered with if the provisions of paragraph *(b)* are complied with.
37	**Wrongful search, access or seizure and restriction on use of instrument device, password of decryption key or information to gain access**	(1) A police official or an investigator who unlawfully and intentionally— *(a)* acts contrary to the authority of— (i) a search warrant issued under section 29(1); or (ii) consent granted in terms of section 31(1); or *(b)* without being authorised thereto under this Chapter or the provision of any other law which affords similar powers to a police official or investigator— (i) searches for, accesses or seizes data, a computer program, a computer data storage medium or any part of a computer system; or (ii) obtains or uses any instrument, device, password, decryption key or other information that is necessary to access data, a computer program, a computer data storage medium or any part of a computer system, is guilty of an offence.
39	**Prohibition on disclosure of information**	(1) No person, investigator, police official, electronic communications service provider, financial institution or an employee of an electronic communications service provider or financial institution may, subject to subsection (2), disclose any information which **[he, she or it has]** they have obtained in the exercise of **[his, her or its]** their powers or the performance of **[his, her or its]** their duties in terms of Chapters 4 or 5 of this Act, except— *(a)* to any other person who of necessity requires it for the performance of **[his or her]** their functions in terms of this Act;

		(b) if **[he or she is]** <u>they are</u> a person who of necessity supplies such information in the performance of **[his or her]** <u>their</u> duties or functions in terms of this Act; *(c)* if it is information which is required in terms of any law or as evidence in any court of law; *(d)* if it constitutes information-sharing between electronic communications service providers, financial institutions, the South African Police Service, competent authorities or any other person or entity which is aimed at preventing, detecting, investigating or mitigating cybercrime: Provided that such information-sharing may not prejudice any criminal investigation or criminal proceedings; or *(e)* to any competent authority in a foreign State which requires it for the prevention, detection, or mitigation of cybercrime, or the institution of criminal proceedings or an investigation with a view to institute criminal proceedings. (2) The prohibition on disclosure of information contemplated in subsection (1) does not apply where the disclosure— **[*(a)* is protected or authorised under the Protected Disclosures Act, 2000, the Companies Act, 2008, the Prevention and Combating of Corrupt Activities Act, 2004, the National Environmental Management Act, 1998, or the Labour Relations Act, 1995;]** <u>*(a)*</u> <u>is authorised in terms of this Act or any other Act of Parliament; or</u> <u>*(b)*</u> <u>reveals a criminal activity.</u>
40	**Interception of indirect, communication, obtaining of real-time communication-related information and archived communication-related u**	(1) The interception of **[data which is]** an indirect communication as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, must take place in terms of a direction issued in terms of section 16(4) or 18(3) of that Act and must, subject to subsection (4), be dealt with further in the manner provided for in that Act. (2) The obtaining of real-time communication-related information as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, on an ongoing basis, as it becomes available must take place in terms of a direction issued in terms of section 17(3) or 18(3) of that Act, and must, subject to subsection (4), be dealt with further in the manner provided for in that Act. (3) An electronic communications service provider who is— *(a)* in terms of section 30(1)*(b)* of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, required to provide an electronic communications service which has the capability to store communication-related information; and *(b)* not required to store communication-related information in terms of a

		directive issued in terms of section 30(2) of that Act, must, in addition to any other obligation imposed by any law, comply with— (i) a real-time communication-related direction contemplated in subsection (2) in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available; (ii) an expedited preservation of data direction contemplated in section 41, in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer; (iii) a preservation of evidence direction contemplated in section 42 in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer; (iv) a disclosure of data direction contemplated in section 44 in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer that was preserved or otherwise stored by the electronic communications service provider; or (v) any order of the designated judge in terms of section 48(6), in terms of which the electronic communications service provider is ordered to— *(aa)* obtain and preserve any real-time communication-related information; or *(bb)* obtain and furnish traffic data. (4) Any indirect communication which is to be intercepted or any real-time communication-related information or traffic data which is to be obtained**, [on an ongoing basis, or archived communication-related information which was obtained and stored, or traffic data which is obtained]** at the request of an authority, court or tribunal exercising jurisdiction in a foreign State must further be dealt with in the manner provided for in an order referred to in section 48(6), which is issued by the designated judge.
41	**Expedited preservation of data direction**	**[(1) A specifically designated police official may, if he or she on reasonable grounds believes that any person, an electronic communications service provider referred to in section 40(3), or a financial institution, is in possession of, is to receive, or is in control of data—** ***(a)* which is relevant to;** ***(b)* which was used or may be used in;** ***(c)* for the purposes of or in connection with;** ***(d)* which has facilitated or may facilitate; or** ***(e)* which may afford evidence of,** **the commission or intended commission of—** **(i) an offence in terms of Part I or Part II of Chapter 2;** **(ii) any other offence in terms of the laws of the Republic, which may be**

		committed by means of, or facilitated by, the use of an article; or **(iii) an offence—** ***(aa)*** **similar to those contemplated in Part I or Part II of Chapter 2; or** ***(bb)*** **substantially similar to an offence recognised in the Republic, which may** **be committed by means of, or facilitated by the use of an article, in a foreign State, issue, with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question, an expedited preservation of data direction to such a person, electronic communications service provider or financial institution.]** (1) A specifically designated police official may– (a) if they believe that there are reasonable grounds that any person, an electronic communications service provider referred to in section 40(3), or a financial institution is— (i) in possession of; (ii) to receive; or (iii) in control of, data as contemplated in paragraph *(a)* of the definition of "article"; and (b) with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question, issue an expedited preservation of data direction to such a person, electronic communications service provider or financial institution. (2) Subsection (1) also applies to— *(a)* archived communication-related information which an electronic communications service provider is no longer required to store due to the fact that the period contemplated in section 30(2)*(a)*(iii) of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, is due to come to an end; or *(b)* any other data which— (i) **[which]** must be stored for a certain period in terms of any other law and that period is due to come to an end; or (ii) **[which]** is stored by an electronic communications service provider which is not real-time communication-related information or archived communication-related information as contemplated in section 1, read with section 30(2) and any directive issued in terms of that section, of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002. (7) A person, electronic communications service provider or financial institution to whom an expedited preservation of data direction, referred to in subsection (1), is addressed may, in writing in the prescribed form and manner, apply to a magistrate in whose area of jurisdiction the person, electronic

		communications service provider or financial institution is situated, for an amendment or the cancellation of the direction concerned on the ground that **[he, she or it]** they cannot timeously or in a reasonable fashion, comply with the direction.
42	**Preservation of evidence direction**	**[(1) A magistrate or judge of the High Court may, on written application by a police official, if it appears to the magistrate or judge, from information on oath or by way of affirmation, as set out in the application, that there are reasonable grounds for believing that any person, electronic communications service provider or financial institution may receive, is in possession of, or is in control of an article—** ***(a)* **relevant to;** ***(b)* which was used or may be used in;** ***(c)* for the purpose of or in connection with;** ***(d)* which has facilitated or may facilitate; or** ***(e)* which may afford evidence of,** **the commission or intended commission of—** **(i) an offence under Part I or Part II of Chapter 2;** **(ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated by the use of an article; or** **(iii) an offence—** ***(aa)* similar to those contemplated in Part I or Part II of Chapter 2; or** ***(bb)* substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated by the use of an article,** **in a foreign State,** **with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question, issue a preservation of evidence direction.]** (1) A magistrate or judge of the High Court, may— *(a)* upon written application by a police official; *(b)* if it appears to the magistrate or judge upon consideration of the information provided under oath or by way of affirmation, as set out in the application, that there are reasonable grounds to believe that any person, electronic communications service provider or financial institution— (i) may receive; (ii) is in possession of; or (iii) is in control of, an article; and *(c)* with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question, issue a preservation of evidence direction.

		(5) A person, electronic communications service provider or financial institution to whom a preservation of evidence direction referred to in subsection (1) is addressed may, in writing in the prescribed form and manner, apply to a magistrate or judge of the High Court in whose area of jurisdiction the person, electronic communications service provider or financial institution is situated for an amendment or the cancellation of the direction concerned on the ground that **[he, she or it]** they cannot timeously or in a reasonable fashion, comply with the direction.
43	**Oral application for preservation of evidence direction**	(1) A police official may orally make an application referred to in section 42(1), **[may be made orally by a police official, if he or she is]** if they are of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application. (3) A magistrate or judge of the High Court may, upon receipt of an oral application made to **[him or her]** them in terms of subsection (1), **[with due regard to the rights, responsibilities and legitimate interest of other persons in proportion to the severity of the offence in question]**, issue the preservation of evidence direction applied for. (6) A magistrate or judge of the High Court who issued a direction under subsection (3) or, if **[he or she is]** they are not available, any other magistrate or judge of the High Court must, upon receipt of a written application **[submitted to him or her]** in terms of subsection (4)*(b)*, reconsider that application whereupon **[he or she]** they may confirm, amend or cancel that preservation of evidence direction.
44	**Disclosure of data direction and search for, access to and seizure of articles subject to preservation of evidence direction**	**[(1) Where—** ***(a)*** **an expedited preservation of data direction or a preservation of evidence direction is in place and it is expedient to obtain data without issuing a search warrant contemplated in section 29(1); or** ***(b)*** **it is otherwise expedient to obtain data without issuing a search warrant contemplated in section 29(1),** **a magistrate or judge of the High Court may, subject to section 4(3) of the Customs and Excise Act, 1964, sections 69(2)*(b)* and section 71 of the Tax Administration Act, 2011 and section 21*(e)* and *(f)* of the Customs Control Act, 2014, on written application by a police official, if it appears to the magistrate or judge from information on oath or by way of affirmation, as set out in the application, that there are reasonable grounds for believing that a person, electronic communications service provider or financial institution, other than the person, electronic communications service provider or financial institution who is suspected of having committed the offence which is being investigated, may receive, is in possession of, or is in control of data which is relevant to or which may afford evidence of the commission or intended commission of—**

		(i) an offence in terms of Part I or Part II of Chapter 2; or **(ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated by the use of an article,** **issue a disclosure of data direction.** **(2) An application contemplated in subsection (1) must—** ***(a)* contain the identity of the police official who applies for the disclosure of data direction;** ***(b)* identify the customer, if known, or the service or communication in respect of whom data is to be provided;** ***(c)* identify the person, electronic communications service provider or financial institution to whom the disclosure of data direction must be addressed;** ***(d)* contain a description of the data which must be provided and the format in which it must be provided;** ***(e)* contain a description of the offence which has been or is being or will probably be committed; and** ***(f)* comply with any supplementary directives relating to applications for expedited disclosure of data, which may be issued by the Chief Justice in terms of section 8(3) of the Superior Courts Act, 2013.** **(3) Upon receipt of an application in terms of subsection (1), a magistrate or judge must satisfy himself or herself—** ***(a)* that there are reasonable grounds for believing that—** **(i) an offence in terms of Part I or Part II of Chapter 2; or** **(ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated by the use of an article,** **has been, is being or will probably be committed or that it is necessary to determine whether such an offence has been so committed; and** ***(b)* that it will be in the interests of justice if a disclosure of data direction is issued.]** (1)*(a)* A police official may, where it is expedient, other than by way of a search for a seizure in terms of a warrant contemplated in section 29(1), to obtain— (i) data which is subject to preservation in terms of an expedited preservation of data direction or a preservation of evidence direction; or (ii) data as contemplated in paragraph *(a)* of the definition of "article", which is— *(aa)* held in a computer system or computer storage medium; or *(bb)* available to a computer system, apply to a magistrate or judge of the High Court for the issuing of a disclosure of data direction. *(b)* An application referred to in paragraph *(a)*(i) must— (i) indicate the identity of the police official who applies for the disclosure of data direction;

		(ii) identify the person, electronic communications service provider or financial institution to whom the disclosure of data direction must be addressed; (iii) be accompanied by a copy of the expedited preservation of data direction or a preservation of evidence direction or any amendment thereof; (iv) contain a description of the data which must be provided and the format in which it must be provided; (v) specify the grounds for believing that the data is an article as contemplated in paragraph *(a)* of the definition of "article"; and (vi) comply with any supplementary directives relating to applications for the disclosure of data, which may be issued by the Chief Justice in terms of section 8(3) of the Superior Courts Act, 2013. *(c)* An application referred to in paragraph *(a)*(ii) must— (i) indicate the identity of the policy official who applies for the disclosure of data direction; (ii) identify the person, electronic communications service provider or financial institution to whom the disclosure of data direction must be addressed; (iii) contain a description of the data which must be provided and the format in which it must be provided; (iv) specific the grounds for believing that the data is an article as contemplated in paragraph *(a)* of the definition of "article"; (v) specify the grounds for believing that the data, in question, is held in a computer system or computer data storage medium or is available to a computer system that is under the control of the person, electronic communications service provider or financial institution, referred to in subparagraph (ii), within the area of jurisdiction of the court; and (vi) comply with any supplementary directives relating to applications for the disclosure of data, which may be issued by the Chief Justice in terms of section 8(3) of the Superior Courts Act, 2013. (2) A magistrate or judge of the High Court may, subject to section 4(2) of the Customs and Excise Act, 1964, sections 69(2)*(b)* and section 71 of the Tax Administration Act, 2011and section 21*(e)* and *(f)* of the Customs Control Act, 2014, on the written application by a police official referred to in subsection (1), if it appears to the magistrate or judge from information on oath or by way of affirmation, as set out in the application— *(a)* that there are reasonable grounds for believing that— (i) data which is subject to preservation in terms of an expedited preservation of data direction or a preservation of evidence direction, is an article as contemplated in paragraph *(a)* of the definition of "article"; or (ii) data, which is an article as contemplated in paragraph *(a)* of the definition of "article", is— *(aa)* held in a computer system or computer data storage medium; or *(bb)* available to a computer system,

		within their area of jurisdiction; and *(b)* that it will be in the interests of justice if a closure of data direction is issued, issue the disclosure of data direction applied for. **[(4)]**(3) A disclosure of data direction must be in the prescribed form and must be served on the person, electronic communications service provider or financial institution affected thereby, in the prescribed manner by a police official. **[(5)]**(4) The disclosure of data direction— *(a)* must direct the person, electronic communications service provider or financial institution to provide data identified in the direction to the extent set out in the direction to an identified police official; *(b)* must specify the format in which the data identified in paragraph *(a)* must be provided; **[*(b)*]***(c)*** must set out the period within which the data identified in paragraph *(a)* must be provided; and **[*(c)*]***(d)*** may specify conditions or restrictions relating to the provision of data authorised therein. **[(6)]**(5) A person, electronic communications service provider or financial institution on whom a disclosure of data direction referred to in subsection **[(5)]**(4) is **[addressed]** served may, in writing in the prescribed form and manner, apply to the magistrate or judge for an amendment or the cancellation of the direction concerned on the ground that **[he or she]** they cannot timeously or in a reasonable fashion comply with the direction. **[(7)]**(6) The magistrate or judge to whom an application is made in terms of subsection **[(6)]**(5) must, as soon as possible after receipt thereof— *(a)* consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application; *(b)* give a decision in respect of the application; and *(c)* if the application is successful, inform the police official of the outcome of the application. **[(8)]**(7) Any data **[which is]** made available in terms of a disclosure of data direction, must be— *(a)* provided to the police official identified in the direction; and *(b)* accompanied by an affidavit in the prescribed form by the person or authorised representative of an electronic communications service provider or financial institution, verifying the authenticity, integrity and reliability of the data that is furnished. **[(9)]**(8) A person, electronic communications service provider or a financial institution who—

		(a) fails to comply with a disclosure of data direction; *(b)* makes a false statement in an application referred to in subsection **[(6)]**(5); or *(c)* fails to comply with subsection **[(8)]**(7); is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment. **[(10)]**(5) *(a)* Any article subject to a preservation of evidence direction that is not ''data'' must be seized in terms of a warrant referred to in section 29(1). *(b)* A police official may, at any time, apply for a search warrant in terms of section 29(1) to search for, access or seize an article (which includes "data") that is or was subject to a preservation of evidence direction.
48	**Foreign requests for assistance and cooperation**	(1) A request by an authority, court or tribunal exercising jurisdiction in a foreign State for the— *(a)* preservation of data or other article; *(b)* seizure of data or other article; *(c)* expedited disclosure of traffic data; *(d)* obtaining of real-time communication-related information or archived communication- related information; or *(e)* interception of indirect communications, must, subject to subsection **[(7)]**(9), be submitted to the designated Point of Contact. (4)*(a)* The National Director of Public Prosecutions must submit the request for assistance, together with **[his or her]** their recommendations, to the Cabinet member responsible for the administration of justice, for **[his or her]** the Cabinet member's approval. *(b)* Upon being notified of the Cabinet member's approval the National Director of Public Prosecutions must forward the request contemplated in subsection (1) to the designated judge for consideration. (5) Where the request relates to the expedited disclosure of traffic data, subsections (3)*(a)*(iv) and (4) do not apply, and the National Director of Public Prosecutions must submit the request for assistance, together with **[his or her]** their recommendations, to the designated judge. (6) Subject to subsections (7) and (8), the designated judge may on receipt of a request referred to in subsection (4) or (5), issue any order which **[he or she deems]** they deem appropriate to ensure that the requested— *(a)* data or other article is preserved in accordance with section 42; *(b)* data or other article is seized on an expedited basis in accordance with section 29 and preserved; *(c)* traffic data is disclosed on an expedited basis in accordance with section 44**[(1)]**(2);

		(d) real-time communication-related information or archived communication-related information, is obtained and preserved; or *(e)* indirect communications are intercepted and preserved, as is specified in the request. (7) The designated judge may only issue an order contemplated in subsection (6), if— *(a)* on the facts alleged in the request, there are reasonable grounds to believe that— (i) an offence substantially similar to the offences contemplated in Part I or Part II of Chapter 2 has been**,** **[or]** is being**,** or will probably be committed; or (ii) any other offence substantially similar to an offence recognised in the Republic, has been**,** **[or]** is being**,** or will probably be committed by means of, or facilitated through the use of an article; and (iii) for purposes of the investigation it is necessary, in the interests of justice, to give an order contemplated in subsection (6); *(b)* the request clearly identifies— (i) the person, electronic communications service provider or financial institution— *(aa)* who or which will receive, is in possession of, or is in control of, the data or other article that must be preserved; or *(bb)* from whose facilities the data, real-time communication-related information, archived communication-related information, indirect communications or traffic data must be obtained or intercepted; (ii) the data or other article which must be preserved; (iii) the data or other article which must be seized on an expedited basis and be preserved; (iv) the traffic data which must be disclosed on an expedited basis; (v) the real-time communication-related information or archived communication-related information, which is to be obtained; or (vi) the indirect communications, which are to be intercepted; *(c)* the request is, where applicable, in accordance with— (i) any treaty, convention or other agreement to which that foreign State and the Republic are parties or which can be used as a basis for mutual assistance; or (ii) any agreement with any foreign State entered into in terms of section 57; and *(d)* the order contemplated in subsection (6) is in accordance with any applicable law of the Republic. (8) The designated judge may, where **[Where]** a request relates to the expedited disclosure of traffic data **[as contemplated in subsection (6)*(c)*, the designated judge may]**— *(a)* specify conditions or restrictions relating to the disclosure of traffic data as

		[he or she deems] they deem appropriate; or *(b)* refuse to issue an order referred to in subsection (6)*(c)*, if the disclosure of the traffic data **[will, or is likely to,]** may prejudice the sovereignty, security, public safety, or other essential interests of the Republic. (10)*(a)* A specifically designated police official must serve or execute an order contemplated in subsection (6) **[must be served of executed by a specifically designate police official]**. *(b)* The specifically designated police official referred to in paragraph *(a)*, must inform— (i) the designated judge; and (ii) the National Director of Public Prosecutions, in writing, of the fact that an order has been served or executed.
49	**Complying with order of designated judge**	(2) A person, electronic communications service provider or financial institution to whom an order referred to in section 48(6) is addressed may, in writing, apply to the designated judge for an amendment or the cancellation of the order concerned on the ground that **[he, she or it]** they cannot timeously or in a reasonable fashion, comply with the order.
50	**Informing foreign State of outcome of request for mutual assistance and expedited disclosure of traffic data**	(2) Any traffic data **[which is]** made available in terms of an order referred to in section 48(6)*(c)*, must be— *(a)* provided to the designated Point of Contact, in the prescribed manner, for submission to the applicable in authority in a foreign State; and *(b)* accompanied by— (i) a copy of the order referred to in section 48(6); and (ii) an affidavit in the prescribed form by the person or authorised representative of an electronic communications service provider or financial institution, verifying the authenticity, integrity and reliability of the information that is furnished. (3) The **[information referred to in subsection (2)*(a)*, together with the copy of the order and affidavit referred to in subsection (2)*(b)*]** traffic data together with the copy of the order and affidavit referred to in subsection (2)**[*(b)*]**, must be provided to the applicable authority in a foreign State which requested the assistance in terms of section 48(1).
51	**Issuing of direction requesting assistance from foreign State**	(2) A direction contemplated in subsection (1) must specify that— *(a)* there are reasonable grounds for believing that an offence contemplated in **[this Act]** subsection (1)*(a)* or *(b)* has been committed in the Republic or that it is necessary to determine whether such an offence has been committed; *(b)* an investigation in respect thereof is being conducted; and *(c)* for purposes of the investigation it is necessary, in the interests of justice, that— (i) data or other articles specified in the direction be preserved;

		(ii) data or any other article specified in the direction is to be seized on an expedited basis and be preserved; (iii) traffic data specified in the direction, be disclosed on an expedited basis; (iv) real-time communication-related information or archived communication-related information specified in the direction, be obtained and be preserved; or (v) indirect communication, specified in the direction, be intercepted and be preserved, within the area of jurisdiction of a foreign State.
52	**Establishment and functions of designated Point of Contact**	(3)*(a)* The designated Point of Contact must ensure the provision of immediate assistance for the purpose of proceedings or investigations regarding the commission or intended commission of— (i) an offence under Part I or Part II of Chapter 2; (ii) any other offence in terms of the laws of the Republic, which may be committed or facilitated by means of an article; or (iii) an offence— *(aa)* similar to those contemplated in Part I or Part II of Chapter 2; or *(bb)* substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated by the use of an article, in a foreign State. *(b)* The assistance contemplated in subsection (3)*(a)*, includes— (i) the provision of technical advice and assistance; (ii) the facilitation or provision of assistance regarding anything which is authorised under Chapters 4 **[or]** and 5; (iii) the provision of legal assistance; (iv) the identification and location of an article; (v) the identification and location of a suspect; and (vi) cooperation with appropriate authorities of a foreign State.
53	**Proof of certain facts by affidavit**	(1) Whenever any fact established by any examination or process requiring any skill in— *(a)* the interpretation of data; *(b)* the design of, or functioning of data, a computer program, a computer data storage medium or a computer system; *(c)* computer science; *(d)* electronic communications networks and technology; *(e)* software engineering; or *(f)* computer programming, is or may become relevant to an issue at criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 1998, a document purporting to be an affidavit or a solemn or attested declaration made by a person who, in that document, states that **[he or she]** they— (i) *(aa)* **[falls]** fall within a category of persons within the Republic; or

		(bb) is in the service of a body in the Republic or a foreign State, **[designated by the Cabinet member responsible for the administration of justice, by notice in the *Gazette*;]** <u>designated by the Cabinet member responsible for the administration of justice, by notice in the *Gazette*;</u> (ii) possesses relevant qualifications, expertise and experience which **[make him or her]** <u>makes them</u> competent to make the affidavit; and (iii) **[has]** <u>have</u> established such fact by means of an examination or process that is documented in the document, is, upon its mere production at such proceedings, *prima facie* proof of such fact. (5)*(a)* For the purposes of subsection (1), a document purporting to be an affidavit or a solemn or attested declaration made by a person who in that affidavit alleges that **[he or she is]** <u>they are</u> in the service of a body in the Republic or a foreign State designated by the Cabinet member responsible for the administration of justice, by notice in the *Gazette*, has no effect unless <u>it is</u>— (i) it is obtained in terms of an order of a competent court or on the authority of a government institution of the foreign State concerned, as the case may be; and (ii) it is authenticated— *(aa)* in the manner prescribed in the rules of court for the authentication of documents executed outside the Republic; or *(bb)* by a person and in the manner contemplated in section 7 or 8 of the Justices of the Peace and Commissioners of Oaths Act, 1963. *(b)* The admissibility and evidentiary value of an affidavit contemplated in paragraph *(a)* are not affected by the fact that the form of the oath, confirmation or attestation thereof differs from the form of the oath, confirmation or attestation prescribed in the Republic. *(c)* A court before which an affidavit or a solemn or attested declaration contemplated in paragraph *(a)* is placed may, in order to clarify any obscurities in the said affidavit, order that a supplementary affidavit or a solemn or attested declaration be submitted or that oral evidence be heard: Provided that oral evidence may only be heard if the court is of the opinion that it is in the interests of the administration of justice and that a party to the proceedings would be prejudiced materially if oral evidence is not heard.
54	**Obligations of electronic communications service providers and financial institutions**	(1) An electronic communications service provider or financial institution that is aware or becomes aware that its **[computer system]** <u>electronic communications service or electronic communications network</u> is involved in the commission of any category or class of offences provided for in Part I of 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.
55	**Capacity to detect, prevent and investigate cybercrimes**	(3) The Cabinet Member responsible for policing must, at the end of each financial year, submit a report to Parliament regarding— *(a)* progress made with the implementation of this section; *(b)* the number of— (i) offences provided for in Part I or Part II of Chapter 2, which were reported to the South African Police **[Services]** Service; (ii) cases which were, in terms of subparagraph (i), reported to the South African Police Service which resulted in criminal prosecutions; and (iii) cases where no criminal prosecutions were instituted after a period of 18 months after a case was, in terms of subparagraph (i), reported to the South African Police Service; and *(c)* the number of members of the South African Police Service who received training as contemplated in subsection (1)*(b)* and *(c)*.
59	**Regulations**	(1) The Cabinet member responsible for the administration of justice **[must make regulations]**— *(a)* must make regulations to prescribe the— (i) form and manner of the application contemplated in section 20(1); (ii) form of the order contemplated in section 20(3); (iii) **[form and]** manner of serving the order contemplated in section 20(4); (iv) form and manner of the application contemplated in section 20(6); (v) **[form and]** manner in which the court may subpoena a person as contemplated in section 20(8); (vi) form of the direction and affidavit and manner to furnish information to a court as contemplated in section 21(1)*(b)*; (vii) manner of serving a direction as contemplated in section 21(2); (viii) manner of, and the form of, the affidavit to apply for an extension of the time period or cancellation of the direction as contemplated in section 21(3)*(b)*; (ix) manner for requesting additional information as contemplated in section 21(4)*(b)*; (x) form and manner of informing an electronic communications service provider or person of the outcome of application as contemplated in section 21(4)*(d)*; (xi) tariffs of compensation payable to an electronic communications service provider as contemplated in section 21(6); (xii) form of the order and manner of service of the order as contemplated in section 22(3);

		(xiii) form and manner of the application contemplated in section 22(5); (xiv) form and manner in which the court may subpoena a person as contemplated in section 22(7); **[(xiii)]**(xv) the form of the expedited preservation of data direction and manner of service as contemplated in section 41(3); **[(xiv)]**(xvi) form and manner for the making of an application contemplated in section 41(7); **[(xv)]**(xvii) form of the preservation of evidence direction and manner of service contemplated in section 42(2); **[(xvi)]**(xviii) form and manner for an application to set aside a preservation of evidence direction as contemplated in section 42(5); **[(xvii)]**(xix) form of the disclosure of data direction and manner of service as contemplated in section 44**[(4)]**(3); **[(xviii)]**(xx) form and manner of an application for the amendment or setting aside of a disclosure of data direction as contemplated in section 44**[(6)]**(5); **[(xix)]**(xxi) form of the affidavit contemplated in section 44**[(8)]**(7)*(b)*; **[(xx)]**(xxii) manner in which traffic data must be submitted to the designated Point of Contact as contemplated in section 50(2). **[(xxi)]**(xxiii) form of the affidavit contemplated in section 50(2)*(b)*(ii); and **[(xxii)]**(xxiv)form of the direction contemplated in section 51(1); and *(b)* may make regulations which is not inconsistent with this Act or any other law to prescribe any matter which in terms of this Act may be prescribed or which may be necessary or expedient to prescribe in order to achieve or promote the objects of this Act.
60	**Short title and commence-ment**	(1) This Act is called the Cybercrimes Act, **[2019]** 2020, and comes into operation on a date fixed by the President by proclamation in the *Gazette*.
Schedule *(Section 58)* **LAWS REPEALED OR AMENDED**		
Act No. 51 of 1977	**Criminal Procedure Act, 1977**	(a) The addition of the following items to Schedule 5: "A contravention of sections 8, 9 or 10 of the Cybercrimes Act, **[2019]** 2020— (a) involving amounts of more than R500 000,00; (b) involving amounts of more than R100 000,00, if it is proven that the offence was committed— (i) by a person, group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; (ii) by a person or with the collusion or assistance of another

		person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offences in question were committed; or (iii) by any law enforcement officer— (aa) involving amounts of more than R10 000; or (bb) as a member of a group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or (cc) with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offences in question were committed. A contravention of section 11(2) of the Cybercrimes Act, **[2019]** 2020.".
Act No. 65 of 1996	**Films and Publications Act, 1996**	**[(*a*) The amendment of section 1 by the substitution for the definition of " child pornography" of the following definition: "child pornography" means "child pornography" as defined in section 1 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act No. 32 of 2007).** **(*b*)]** The deletion of sections 24B**[, 27A and 30B(1)(*b*)]**.
Act No. 105 of 1997	**Criminal Law Amendment Act, 1997**	The addition of the following item to Part II of Schedule 2: of the following Part: "A contravention of sections 8, 9 or 10 of the Cybercrimes Act, **[2019]** 2020— (a) involving amounts of more than R500 000,00; (b) involving amounts of more than R100 000,00, if it is proven that the offence was committed— (i) by a person, group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; (ii) by a person or with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offences in question were committed; or (iii) if it is proven that the offence was committed by any law enforcement officer—

		(aa) involving amounts of more than R10 000; or (bb) as a member of a group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or (cc) with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offences in question were committed.". **[A contravention of section 11(2) of the Cybercrimes Act, 2020.".]**
Act No. 70 of 2002	**Regulation of Interception of Communications and Provision of Communication related Information Act, 2002**	*(a)* The amendment of section 1 by the substitution for paragraph *(a)* of the definition of "serious offence" of the following paragraph: "*(a)* offence mentioned in **[the]** Schedule 1; or". *(b)* The amendment of section 4 by the addition of the following subsection: "(3) Notwithstanding subsection (2), a law enforcement officer or a person who is authorised in terms of the Criminal Procedure Act, 1977, the Cybercrimes Act, **[2019]** 2020 or any other law to engage or to apprehend a suspect or to enter premises in respect of the commission of or suspected commission of any offence, may during the apprehension of the suspect or during the time that he or she is lawfully on the premises, record what he or she observes or hears if— (*a*) the recording relates directly to the purpose for which the suspect was apprehended or the law enforcement officer or person entered the premises; and (*b*) the law enforcement officer or person has— (i) identified himself or herself as such; and (ii) verbally informed any person concerned that his or her direct communications are to be recorded, before such recording is made.". **[*(b)*]***(c)*** The substitution for subsection (4) of section 17 of the following subsection: "(4) A real-time communication-related direction may only be issued if it appears to the designated judge concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that— *(a)* a serious offence or an offence mentioned in Schedule II has been or is being or will probably be committed; *(b)* the gathering of information concerning an actual threat

to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

(c) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

(d) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime, an offence mentioned in Schedule II or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in—

(i) accordance with an international mutual assistance agreement; or

(ii) the interests of the Republic's international relations or obligations; or

(e) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence, or an offence mentioned in Schedule II or is or could probably be the proceeds of unlawful activities is necessary,

and that the provision of real-time communication-related information is necessary for purposes of investigating such offence or gathering such information.".

(d) The substitution for subsection (4) of section 19 of the following subsection:

"(4) An archived communication-related direction may only be issued if it appears to the judge of a High Court, regional court magistrate or magistrate concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that—

(*a*) a serious offence or an offence mentioned in Schedule II has been or is being or will probably be committed;

(*b*) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

(*c*) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

(*d*) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in

connection with, or in the form of, the interception of communications relating to organised crime , an offence mentioned in Schedule II or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in—

(i) accordance with an international mutual assistance agreement; or

(ii) the interests of the Republic's international relations or obligations; or

(e) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence, or an offence mentioned in Schedule II or is or could probably be the proceeds of unlawful activities is necessary,

and that the provision of archived communication-related information is necessary for purposes of investigating such offence or gathering such information.".

[*(c)*]*(e)* The renaming of the Schedule to the Act as "Schedule I" and the addition of the following items:

"**15.** Any offence contemplated in sections 17, 18, 19A or 20 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act No. 32 of 2007).

16. Any offence contemplated in—

(a) section 8, 9(1) or (2) or 10 of the Cybercrimes Act, **[2019]** 2020, which involves an amount of R200 000, 00 or more; or

(b) section 11(1) or (2) or 17 (in so far as the section relates to the offences referred to in section 11(1) or (2) of that Act).".

[*(e)*]*(f)* The addition of the following Schedule after Schedule I:

"**Schedule II**

1. Any offence referred to in—

(a) sections 3(1), 5, 6, 7(1), 8, 9(1) or (2), or 10; or

(b) section 17 (in so far as the section relates to the offences referred to in paragraph *(a)*),

of the Cybercrimes Act,**[2019]** 2020, which involves an amount of R50 000, 00 or more.

2. Any offence which is substantially similar to an offence referred to in item 1 which is or was committed in a foreign State, which involves an amount of R50 000, 00 or more.".

Act No. 32 of 2007	**Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007**	**[*(a)* The Index to the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007,is hereby amended by—** **(i) the substitution for the heading to Part 3 of Chapter 2 of the following heading:** **"*Persons 18 years or older: Compelling or causing persons 18 years or older to witness sexual offences, sexual acts or self-masturbation, exposure or display of or causing exposure or display of genital organs, anus or female breasts (''flashing''), child pornography to persons 18 years <u>or older, harmful disclosure of pornography</u> or engaging sexual services of persons 18 years or older";*** **(ii) the insertion after item 10 of the following item:** **"<u>10A. Harmful disclosure of pornography</u>";** **(iii) the substitution for the heading to Part 2 of Chapter 3 of the following heading:** **"*Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of <u>child pornography</u> or pornography to children, child pornography and using children for pornographic purposes or benefiting from child pornography''*; and** **(iv) the insertion after item 19 of the following item:** **"<u>19A. Offences relating to child pornography</u>".** ***(b)* The amendment of section 1—** **(i) by the substitution for the definition of "child pornography" of the following definition:** **"child pornography" means any image, however created, or any description or presentation of a person, real or simulated, who is, or who is realistically depicted or described or presented as being, under the age of 18 years, of an explicit or sexual nature, whether such image or description or presentation is intended to stimulate erotic or aesthetic feelings or not, including any such image, <u>presentation</u> or description of such person—** ***(a)* engaged in an act that constitutes a sexual offence;** ***(b)* engaged in an act of sexual penetration;** ***(c)* engaged in an act of sexual violation;** ***(d)* engaged in an act of self-masturbation;** ***(e)* displaying the genital organs of such person in a state of arousal or stimulation;** ***(f)* unduly displaying the genital organs or anus of such person;** ***(g)* displaying any form of stimulation of a sexual nature of such person's breasts;** ***(h)* engaged in sexually suggestive or lewd acts;** ***(i)* engaged in or as the subject of sadistic or masochistic acts of a sexual nature;**

		(j) **engaged in any conduct or activity characteristically associated with sexual intercourse;** ***(k)*** **showing or describing such person—** **(i) participating in, or assisting or facilitating another person to participate in; or** **(ii) being in the presence of another person who commits or in any other manner being involved in, any act contemplated in paragraphs *(a)* to *(j)*; or** ***(l)*** **showing or describing the body, or parts of the body, of such person in a manner or in circumstances which, within the context, violate or offend the sexual integrity or dignity of that person or any category of persons under 18 or is capable of being used for the purposes of violating or offending the sexual integrity or dignity of that person, any person or group or categories of persons;"; and** **(ii) by the insertion after the definition of "Director of Public Prosecutions" of the following definition:** **"<u>electronic communications service provider" means any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005;</u>".** ***(c)*** **Chapter 2 is hereby amended by—** **(i) the substitution for the heading to Part 3 of Chapter 2 of the following heading:** **"*Persons 18 years or older: Compelling or causing persons 18 years or older to witness sexual offences, sexual acts or self-masturbation, exposure or display of or causing exposure or display of genital organs, anus or female breasts (''flashing''), child pornography to persons 18 years or older, <u>harmful disclosure of pornography</u> or engaging sexual services of persons 18 years or older"*;** **and** **(ii) by the insertion for the following section after section 10:** **"Harmful disclosure of pornography** **<u>10A. (1) A person ("A") who unlawfully and intentionally discloses or causes the disclosure of pornography in which a person 18 years or older ("B") appears or is described and such disclosure—</u>**

		(a) **takes place without the consent of B; and** ***(b)*** **causes any harm, including mental, psychological, physical, social or economic harm, to B or any member of the family of B or any other person in a close relationship to B,** **is guilty of the offence of harmful disclosure of pornography.** **(2) A person ("A") who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1) and such threat causes, or such disclosure could reasonably be expected to cause, any harm referred to in subsection (1)*(b)*, is guilty of the offence of threatening to disclose pornography that will cause harm.** **(3) A person (''A'') who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1), for the purposes of obtaining any advantage from B or any member of the family of B or any other person in a close relationship to B, is guilty of the offence of harmful disclosure of pornography related extortion.** **(4) *(a)* Any person who lays a charge with the South African Police Service that an offence contemplated in subsections (1), (2) or (3) has allegedly been committed against him or her, may on an *ex parte* basis, in the prescribed form and manner, apply to a magistrate's court for an order—** **(i) to prohibit any person to disclose or cause the disclosure of pornography as contemplated in subsections (1), (2) or (3); or** **(ii) ordering an electronic communications service provider or person in control of a computer system to remove or disable access to the pornography in question.** ***(b)*** **The court must as soon as is reasonably possible consider an application submitted to it in terms of paragraph *(a)* and may, for that purpose consider any additional evidence it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of proceedings.** ***(c)*** **The court may, for purposes of paragraph *(b)*, in the prescribed form and manner cause to be subpoenaed any person as a witness at those**

		proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case. ***(d)* If the court is satisfied that there is *prima facie* evidence that the pornography in question constitutes an offence as contemplated in subsection (1), (2) or (3), the court may issue the order referred to in paragraph *(a)*, in the prescribed form.** ***(e)* The order must be served on the person referred to in paragraph *(a)*(i) or electronic communications service provider or person referred to in paragraph *(a)*(ii), in the prescribed form and manner: Provided, that if the court is satisfied that the order cannot be served in the prescribed form and manner, the court may make an order allowing service to be effected in the manner specified in that order.** ***(f)* An order referred to in paragraph *(d)* is of force and effect from the time it is issued by the court and the existence thereof has been brought to the attention of the person or electronic communications service provider.** ***(g)* Any person or electronic communications service provider who fails to comply with an order referred to in paragraph *(d)* is guilty of an offence.** ***(h)* Any person who is subpoenaed in terms of paragraph *(c)* to attend proceedings and who fails to—** (i) attend or to remain in attendance; (ii) appear at the place and on the date and at the time to which the proceedings in question may be adjourned; (iii) remain in attendance at those proceedings as so adjourned; or (iv) produce any book, document or object specified in the subpoena, is guilty of an offence.** ***(i)* The provisions in respect of appeal and review as provided for in the Magistrates' Courts Act, 1944 (Act No. 32 of 1944), and the Superior Courts Act, 2013 (Act No. 10 of 2013), apply to proceedings in terms of this subsection.** **(5) Whenever a person is—** ***(a)* convicted of an offence in terms of subsections (1), (2) or (3); or** ***(b)* acquitted of an offence in terms of**

		subsections (1), (2) or (3), **and evidence produced at the trial proves that the person engaged in, or attempted to engage in, harassment as contemplated in the Protection from Harassment Act, 2011 (Act No. 17 of 2011), the trial court may, after holding an enquiry, issue a protection order as contemplated in section 9(4) of the Protection from Harassment Act, against the person, whereafter the provisions of that Act shall apply with the necessary changes required by the context.** **(6) A court must, on convicting a person of the commission of an offence contemplated in subsection (1), (2) or (3) order—** ***(a)* **that person to refrain from further making available, broadcasting or distributing the data message contemplated in subsection (1), (2) or (3) which relates to the charge on which he or she is convicted;** ***(b)* **that person or any other person to destroy the data message in question or any copy of the data message; or** ***(c)* **an electronic communications service provider or person in control of a computer system to remove or disable access to the data message in question.** **(7) The order referred to in subsection (6)*(b)*, in so far as it relates to a person other than the accused, and (6)*(c)* must be served on the person or electronic communications service provider or person in control of a computer system in the prescribed form and manner: Provided, that if the trial court is satisfied that the order cannot be served in the prescribed form and manner, the court may make an order allowing service to be effected in the manner specified in that order.** **(8) Any person contemplated in subsection (6)*(a)* or *(b)* or an electronic communications service provider or person in control of a computer system as contemplated in subsection (6)*(c)* who fails to comply with an order referred to in subsection (7), is guilty of an offence.** **(9) For purposes of subsection (5), a "trial court" means—** ***(a)* **a magistrate's court established under section 2(1)*(f)*(i) of the Magistrates' Courts Act, 1944 (Act No. 32 of 1944);**

		(b) **a court for a regional division established under section 2(1)*(g)*(i) of the Magistrates' Courts Act, 1944; or** ***(c)*** **a High Court referred to in section 6(1) of the Superior Courts Act, 2013 (Act No. 10 of 2013).** **(10) Section 21 of the Cybercrimes Act, 2020, applies with the necessary changes required by the context to an application for a protection order in terms of subsection (4).".** ***(d)*** **Chapter 3 is hereby amended—** **(i) by the substitution for the heading to Part II of Chapter 3 of the following heading:** ***''Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of child pornography or pornography to children, offences relating to child pornography and using children for pornographic purposes or benefiting from child pornography"*;** **(ii) by the insertion of the following section after section 19 of the Act:** **"Offences relating to child pornography** **19A. (1) Any person who unlawfully and intentionally creates, makes or produces child pornography, is guilty of an offence.** **(2) Any person who unlawfully and intentionally, in any manner knowingly assists in, or facilitates the creation, making or production of child pornography, is guilty of an offence.** **(3) Any person who unlawfully and intentionally possesses child pornography is guilty of an offence.** **(4) Any person who unlawfully and intentionally, in any manner—** ***(a)*** **distributes;** ***(b)*** **makes available;** ***(c)*** **transmits;** ***(d)*** **offers for sale;** ***(e)*** **sells;** ***(f)*** **offers to procure;** ***(g)*** **procures;** ***(h)*** **accesses;** ***(i)*** **downloads; or** ***(j)*** **views,** **child pornography, is guilty of an offence.** **(5) Any person who unlawfully and intentionally, in any manner knowingly assists in, or facilitates the—**

		(a) **distribution;** ***(b)*** **making available;** ***(c)*** **transmission;** ***(d)*** **offering for sale;** ***(e)*** **selling;** ***(f)*** **offering to procure;** ***(g)*** **procuring;** ***(h)*** **accessing;** ***(i)*** **downloading; or** ***(j)*** **viewing,** **of child pornography, is guilty of an offence.** **(6) Any person who unlawfully and intentionally advocates, advertises, encourages or promotes—** ***(a)*** **child pornography; or** ***(b)*** **the sexual exploitation of children;** **is guilty of an offence.** **(7) Any person who unlawfully and intentionally processes or facilitates a financial transaction, knowing that such transaction will facilitate a contravention of subsections (1) to (6), is guilty of an offence.** **(8) Any person who, having knowledge of the commission of any offence referred to in subsections (1) to (7), or having reason to suspect that such an offence has been or is being committed and unlawfully and intentionally fails to—** ***(a)*** **report such knowledge or suspicion as soon as possible to the South African Police Service; or** ***(b)*** **furnish, at the request of the South African Police Service, all particulars of such knowledge or suspicion,** **is guilty of an offence.** **(9) An electronic communications service provider that is aware or becomes aware that its electronic communications system or service is used or involved in the commission of any offence provided for in subsections (1) to (7), must—** ***(a)*** **immediately report the offence to the South African Police Service;** ***(b)*** **preserve any information which may be of assistance to the law enforcement agencies in investigating the offence; and** ***(c)*** **take all reasonable steps to prevent access to the child pornography by any person.";** **(iii) the amendment of section 20, by the addition of the following subsections:** **"(3) Any person who unlawfully and intentionally—**

		(a) **attends; or** ***(b)*** **views,** **a live performance involving child pornography, is guilty of the offence of attending or viewing a performance involving child pornography.** **(4) Any person ("A") who unlawfully and intentionally recruits a child complainant ("B"), with or without the consent of B, whether for financial or other reward, favour or compensation to B or a third person ("C") or not, for purposes of—** ***(a)*** **creating, making or producing any image, publication, depiction, description or sequence in any manner whatsoever of child pornography, is guilty of the offence of recruiting a child for child pornography; or** ***(b)*** **participating in a live performance involving child pornography, as contemplated in subsection (3), is guilty of the offence of recruiting a child for participating in a live performance involving child pornography."; and** ***(e)*** **the amendment of section 56A, by the addition of the following subsections:** **"(3)*(a)* Any person who contravenes the provisions of section 10A(1) or (2) is liable, on conviction to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.** ***(b)*** **Any person who contravenes the provisions of section 10A(3) is liable, on conviction to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.** ***(c)*** **Any person or electronic communications service provider who contravenes the provisions of subsection 10A(4)*(g)* is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.** ***(d)*** **Any person who contravenes the provisions of subsection 10A(4)*(h)* is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.** ***(e)*** **Any person or electronic communications service provider who contravenes the provisions of section 10A(8), is liable on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.** **(4) Any person who contravenes the provisions of section 19A(3), (4)*(f), (g), (h), (i)* or *(j)*, or (5)*(f), (g), (h), (i)* or *(j)* is liable—** ***(a)*** **in the case of a first conviction, to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment;**

		_(b)_ in the case of a second conviction, to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment; or **_(c)_ in the case of a third or subsequent conviction, to a fine or to imprisonment for a period not exceeding 15 years or to both such fine and imprisonment.** **(5) Any person who contravenes the provisions of section 19A(4)_(a), (b), (c), (d)_, or _(e)_, (5)_(a), (b), (c), (d)_ or _(e)_, (6) or 20(3), is liable—** **_(a)_ in the case of a first conviction, to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment; or** **_(b)_ in the case of a second and subsequent conviction, to a fine or to imprisonment for a period not exceeding 15 years or to both such fine and imprisonment.** **(6) Any person who contravenes the provisions of section 19A(7), is liable—** **_(a)_ in the case of a first conviction, to a fine of R1 000 000 or to imprisonment for a period not exceeding 5 years, or to both such fine and imprisonment;** **_(b)_ in the case of a second or subsequent conviction, to a fine of R 2000 000 or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.** **(7) Any person who contravenes the provisions of section 19A(8), is liable, on conviction to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.** **(8) Any electronic communications service provider who contravenes the provisions of section 19A(9), is liable, on conviction to a fine not exceeding R1 000 000 or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.".]** (_a_) The Index to the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007, is hereby amended by— (i) the insertion of the following Part and items after item 11: "***Part 3A*** *Persons 18 years or older: Harmful disclosure of pornography and orders to protect complainant against the harmful effects of disclosure of pornography* 11A Harmful disclosure of pornography 11B Orders to protect complainant complainant against harmful disclosure of pornography 11C Electronic communications service provider to furnish particulars to court 11D Orders on finalisation of criminal proceedings"; (ii) the substitution for the heading to Part 2 of Chapter 3 of the following

heading:

''Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of child pornography or pornography to children, child pornography and using children for pornographic purposes or benefiting from child pornography''; and

(iii) the insertion after item 19 of the following item:

"19A. Offences relating to child pornography".

(*b*) The amendment of section 1—

(i) by the insertion, after the definition of "Director of Public Prosecutions" of the following definitions:

""**disclose**" in relation to the harmful disclosure of pornography contemplated in section 11A, includes—

(*a*) to send the pornography to a person who is the intended recipient of the electronic communication or any other person;

(*b*) to store the pornography on an electronic communications network, where the pornography can be viewed, copied or downloaded; or

(*c*) to send or otherwise make available to a person, a link to the pornography that has been stored on an electronic communication network, where the pornography can be viewed, copied or downloaded;

"**Electronic Communications Act**" means the Electronic Communications Act, 2005 (Act No. 36 of 2005);

"**electronic communications identity number**" means a technical identification label which represents the origin or destination of electronic communications traffic;

"**electronic communications network**" means an "electronic communications network" as defined in section 1 of the Electronic Communications Act, and includes a computer system;

"**electronic communications service**" means any service which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services as defined in section 1 of the Electronic Communications Act, 2005;

"**electronic communications service provider**" means—

(*a*) any person who provides an electronic communications service to the public, sections of the public, the State, or the subscribers to such service, under and in accordance with an electronic communications service licence issued to that person in terms of the Electronic Communications Act, 2005, or who is deemed to be licensed or exempted from being licensed as such in terms of that Act; and

(*b*) a person who has lawful authority to control the operation or use of a private electronic communications network used primarily for providing electronic communications services for the owner's own

use and which is exempted from being licensed in terms of the Electronic Communications Act, 2005;"; and

(ii) by the insertion, after the definition of "genital organs" of the following definitions:

""**host**" means to store information on an electronic communications network that is used to provide an electronic communications service, where it can be viewed, copied or downloaded.; and

"live performance involving child pornography" means an event where a child is used to create, make or produce child pornography;"**.**

(*c*) The following Part and sections are hereby inserted in Chapter 2 after section 11:

"***Part 3A***

Persons 18 years or older: Harmful disclosure of pornography and orders to protect complainant against the harmful effects of disclosure of pornography

Harmful disclosure of pornography

11A. (1) A person ("A") who unlawfully and intentionally discloses or causes the disclosure of pornography in which a person ("B") appears or is described and such disclosure—

(*a*) takes place without the consent of B; and

(*b*) causes any harm, including mental, psychological, physical, social or economic harm, to B or any member of the family of B or any other person in a close relationship to B,

is guilty of the offence of disclosure of pornography that causes harm.

(2) A person ("A") who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1) and such threat causes, or such disclosure could reasonably be expected to cause, any harm referred to in subsection (1)(*b*), is guilty of the offence of threatening to disclose pornography that will cause harm.

(3) A person ("A") who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1), for the purposes of obtaining any advantage from B or any member of the family of B or any other person in a close relationship to B, is guilty of the offence of harmful disclosure of pornography related extortion.

Orders to protect complainant against harmful disclosure of pornography

11B. (1) A complainant (hereinafter referred to as the applicant) who lays a charge with the South African Police Service that an offence contemplated in section 11A(1), (2) or (3) has allegedly been committed

		against his or her, may on an *ex parte basis* in the prescribed form and manner, apply to a magistrate's court for a protection order pending the finalisation of the criminal proceedings to— (*a*) prohibit any person to disclose, or cause the disclosure or threaten the applicant with the disclosure or causing the disclosure of pornography which relates to the charge; or (*b*) order an electronic communications service provider whose electronic communications service is used to host or disclose the pornography which relates to the charge, to remove or disable access to such pornography. (2) The court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (1) and may, for that purpose consider any additional evidence it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of proceedings. (3) If the court is satisfied that there is — (*a*) *prima facie* evidence that an offence referred to in section 11A(1), (2) or (3), has allegedly been committed against the applicant; (*b*) reasonable grounds to believe that a person referred to in subsection (1)(*a*), disclosed or caused the disclosure or threatened the applicant with the disclosure or causing the disclosure of such pornography; or (*c*) reasonable grounds to believe that the electronic communications service of the electronic communications service provider is used to host or disclose such pornography, the court may, subject to such conditions as the court may deem fit, issue the order referred to in subsection (1), in the prescribed form. (4) The order, referred to in subsection (3), must be served on the person referred to in subsection (1)(*a*) or electronic communications service provider, referred to in subsection (1)(*b*), in the prescribed ~~form and~~ manner: Provided, that if the court is satisfied that the order cannot be served in the prescribed ~~form and~~ manner, the court may make an order allowing service to be effected in the form or manner specified in that order. (5) An order referred to in subsection (3) is of force and effect from the time it is issued by the court and the existence thereof has been brought to the attention of the person referred to in subsection (1)(*a*) or electronic communications service provider referred to in subsection (1)(*b*). (6) A person referred to in subsection (1)(*a*), other than the person who is accused of having committed the offence in question, or an electronic communications service provider, referred to in subsection (1)(*b*) may, within 14 days after the order has been served on him, her or it in terms of subsection (4) or within such further period as the court may allow, upon notice to the magistrate's court concerned, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection (3).

(7) (*a*) The court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (6) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which ~~shall~~ must form part of the record of the proceedings.

(*b*) The court may if good cause has been shown for the variation or setting aside of the protection order, issue an order to this effect.

(8) The court may, for purposes of subsections (2) and (7), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.

(9) A person referred to in subsection (1)(*a*) or electronic communications service provider, referred to in subsection (1)(*b*), that fails to comply with an order referred to in subsection (3) or any variation thereof, is guilty of an offence.

(10) Any person who is subpoenaed in terms of subsection (8) to attend proceedings and who fails to—

(*a*) attend or to remain in attendance;

(*b*) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;

(*c*) remain in attendance at those proceedings as so adjourned; or

(*d*) produce any book, document or object specified in the subpoena,

is guilty of an offence.

(11) The provisions in respect of appeal and review as provided for in the Magistrates' Courts Act, 1944, and the Superior Courts Act, 2013, apply to proceedings in terms of this section.

(12) Sections 8 and 9(3) of the Protection from Harassment Act, 2011 (Act No. 17 of 2011), applies with the necessary changes required by the context to proceedings contemplated in subsections (2) and (7).

—

Electronic communications service provider to furnish particulars to court

11C. (1) If an application for a protection order is made in terms of section 11B(1) and the court is satisfied in terms of section 11B(3) that a protection order must be issued and the particulars of the person referred to in section 11B(1)(*a*) or the electronic communications service provider, referred to in section 11B(1)(*b*), is not known, the court may—

(*a*) adjourn the proceedings to any time and date on the terms and conditions which the court deems appropriate; and

(*b*) issue a direction in the prescribed form, directing an electronic communications service provider that is believed to be able to furnish such particulars, to furnish the court in the prescribed manner by

means of an affidavit in the prescribed form with—

(i) the electronic communications identity number from where such pornography originated;

(ii) the name, surname, identity number and address of the person to whom the electronic communications identity number has been assigned;

(iii) any information which indicates that such a threat to disclose or cause the disclosure of pornography was or was not sent from the electronic communications identity number of the person to the electronic communications identity number of the applicant;

(iv) any information that is available to an electronic communications service provider that may be of assistance to the court to identify the person referred to in section 11B(1)(*a*) or the electronic communications service provider referred to in section 11B(1)(*b*), which provides a service to that person;

(v) any information that is available to an electronic communications service provider which—

(*aa*) confirms whether or not its electronic communications service is used to host or disclose such pornography; or

(*bb*) may be of assistance to the court to identify the electronic communications service provider whose service is used to host or disclose such pornography; and

(vi) an assessment whether or not the electronic communications service provider is in a position—

(*aa*) to remove such pornography or a link to such pornography; or

(*bb*) to disable access to such pornography or a link to such pornography.

(2) If the court issues a direction in terms of subsection (1) the court must direct that the direction be served on the electronic communications service provider in the prescribed manner: Provided, that if the court is satisfied that the direction cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.

(3) (*a*) The information referred to in subsection (1)(*b*) must be provided to the court within five ordinary court days from the time that the direction is served on an electronic communications service provider.

(*b*) An electronic communications service provider on which a direction is served, may in the prescribed manner by means of an affidavit in the prescribed form apply to the court for—

(i) an extension of the period of five ordinary court days referred to in paragraph (*a*) for a further period of five ordinary court days on the grounds that the information cannot be provided timeously; or

(ii) the cancellation of the direction on the grounds that—

(*aa*) it does not provide an electronic communications service to the applicant or the person referred to in section 11B(1)(*a*);

		(*bb*) the requested information is not available in the records of the electronic communications service provider; or (*cc*) its service is not used to host or disclose such pornography. (4) After receipt of an application in terms of subsection (3)(*b*), the court— (*a*) must consider the application; (*b*) may, in the prescribed manner, request such additional evidence by way of affidavit from the electronic communications service provider as it deems fit; (*c*) must give a decision in respect thereof; and (*d*) must inform the electronic communications service provider in the prescribed form and manner of the outcome of the application. (5) (*a*) The court may, on receipt of an affidavit from an electronic communications service provider which contains the information referred to in subsection (1)(*b*), consider the issuing of a protection order in terms of section 11B(3) against the person or electronic communications service provider on the date to which the proceedings have been adjourned. (*b*) Any information furnished to the court in terms of subsection (1)(*b*) forms part of the evidence that a court may consider in terms of section11B(3). (6) The Cabinet member responsible for the administration of justice may, by notice in the *Gazette*, prescribe reasonable tariffs of compensation payable to electronic communications service providers for providing the information referred to in subsection (1)(*b*). (7) Any electronic communications service provider or employee of an electronic communications service provider who— (*a*) fails to furnish the required information within five ordinary court days from the time that the direction is served on such electronic communications service provider to a court in terms of subsection (3)(*a*) or such extended period allowed by the court in terms of subsection (3)(*b*); or (*b*) makes a false statement in an affidavit referred to in subsection (1)(*b*) or (3)(*b*) in a material respect, is guilty of an offence. **Orders on finalisation of criminal proceedings** **11D.** (1) The trial court, on convicting a person of any offence referred to in section 11A(1), (2) or (3), must order— (*a*) that person to destroy the pornography which relates to the charge on which they are convicted and to submit an affidavit in the prescribed form to the prosecutor identified in the order that the pornography has been so destroyed; or (*b*) an electronic communications service provider whose service is used

		to host or disclose such pornography to remove or disable access to such pornography. (2) The order referred to in subsection (1)(*b*), must be in the prescribed form and must be served on the electronic communications service provider in the prescribed manner: Provided, that if the trial court is satisfied that the order cannot be served in the prescribed form and manner, the court may make an order allowing service to be effected in the form or manner specified in that order. (3) Any person or electronic communications service provider who fails to comply with an order referred to in subsection (1), is guilty of an offence. (4) An electronic communications service provider, may, within 14 days after the order referred to in subsection (1)(*b*) has been served on it in terms of subsection (2), upon notice to the trial court concerned, in the prescribed form and manner apply to the trial court for the setting aside or amendment of the order. (5) (*a*) The trial court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (4) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which shall form part of the record of the proceedings. (*b*) The trial court may if good cause has been shown for the variation or setting aside of the order, issue an order to this effect. (6) The trial court may, for purposes of subsections (5)(*a*), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case. (7) Any person who is subpoenaed in terms of subsection (6) to attend proceedings and who fails to— (*a*) attend or to remain in attendance; (*b*) appear at the place and on the date and at the time to which the proceedings in question may be adjourned; (*c*) remain in attendance at those proceedings as so adjourned; or (*d*) produce any book, document or object specified in the subpoena, is guilty of an offence. (8) For purposes of this section ‘‘trial court’’ means— (*a*) a magistrate’s court established under section 2(1)(*f*)(i) of the Magistrates’ Courts Act, 1944; (*b*) a court for a regional division established under section 2(1)(*g*)(i) of the Magistrates’ Courts Act, 1944; or (*c*) a High Court referred to in section 6(1) of the Superior Courts Act, 2013. (9) Whenever a person is convicted of an offence referred to in section 11A(1), (2) or (3), the trial court must issue an order that the person so convicted must reimburse all expenses reasonably incurred by—

		(*a*) a complainant as a result of any direction issued in terms of section 11C(1)(*b*); or (*b*) an electronic communications service provider to remove or disable access to such pornography, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context, to such order. (*d*) Chapter 3 is hereby amended— (i) by the substitution for the heading to Part II of Chapter 3 of the following heading: ***''Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of child pornography or pornography to children, offences relating to child pornography and using children for pornographic purposes or benefiting from child pornography''***; (ii) amendment of section 17, by the addition of the following subsection: "(7) Any person who unlawfully and intentionally in any manner advocates, advertises, encourages or promotes the sexual exploitation of a child, is guilty of an offence.". (iii) by the insertion of the following section after section 19 of the Act: ''**Offences relating to child pornography** **19A.** (1) Any person who unlawfully and intentionally creates, makes or produces child pornography in any manner, other than by using a child for child pornography as contemplated in section 20(1), is guilty of an offence. (2) Any person who unlawfully and intentionally, in any manner assists in, or facilitates the creation, making or production of child pornography ~~as contemplated in subsection (1)~~, is guilty of an offence. (3) Any person who unlawfully and intentionally possesses child pornography, is guilty of an offence. (4) Any person who unlawfully and intentionally, in any manner— *(a)* distributes; *(b)* makes available; *(c)* transmits; *(d)* offers for sale;

		(e) sells; *(f)* offers to procure; *(g)* procures; *(h)* accesses; *(i)* downloads; or *(j)* views, child pornography, is guilty of an offence. (5) Any person who unlawfully and intentionally, in any manner assists in, or facilitates the— *(a)* distribution; *(b)* making available; *(c)* transmission; *(d)* offering for sale; *(e)* selling; *(f)* offering to procure; *(g)* procuring; *(h)* accessing; *(i)* downloading; or *(j)* viewing, of child pornography, is guilty of an offence. (6) Any person who unlawfully and intentionally processes or facilitates a financial transaction, knowing that such transaction will facilitate a contravention of subsections (1) to (5), is guilty of an offence."; and (iv) by the addition to section 20 of the following subsections: ''(3) Any person who unlawfully and intentionally— *(a)* attends; ~~or~~ *(b)* views; or (c) participates in, a live performance involving child pornography, is guilty of the offence of attending or viewing a performance involving child pornography. (4) Any person (''A'') who unlawfully and intentionally recruits a child complainant (''B''), with or without the consent of B, whether for financial or other reward, favour or compensation to B or a third person (''C'') or not, for purposes of— *(a)* creating, making or producing of child pornography, is guilty of the offence of recruiting a child for child pornography; or *(b)* participating in a live performance involving child pornography, as contemplated in subsection (3), is guilty of the offence of recruiting a child for participating in a live performance involving child pornography.''. *(e)* Section 54 of the Act is amended by the addition of the following subsections: "(3) Any person who, having knowledge of the commission of

any offence referred to in section 19A, or having reason to suspect that such an offence has been or is being or will probably be committed and unlawfully and intentionally fails to—

(*a*) report such knowledge or suspicion as soon as possible to the South African Police Service; or

(*b*) furnish, at the request of the South African Police Service, all particulars of such knowledge or suspicion,

is guilty of an offence.

(4) An electronic communications service provider that is aware or becomes aware that its electronic communications service or electronic communications network is used or involved in the commission of any offence provided for in section 19A, must—

(*a*) immediately report the offence to the South African Police Service;

(*b*) preserve any information which may be of assistance to the South African Police Service in investigating the offence; and

(*c*) take all reasonable steps to prevent access to the child pornography by any person.".

(*f*) Section 56A of the Act is amended by the addition of the following subsections:

''(3) *(a)* Any person who contravenes the provisions of section 11A(1) or (2) is liable, on conviction to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(b) Any person who contravenes the provisions of section 11A(3) is liable, on conviction to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(c) Any person or electronic communications service provider that is convicted of an offence referred to in section 11B(9) or (10), is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(d) Any person or electronic communications service provider that is convicted of an offence referred to in section 11C(7), is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(*e*) Any person or electronic communications service provider that is convicted of an offence referred to in section 11D(3) or (7), is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(4) Any person who contravenes the provisions of section 19A(3), (4)*(f), (g), (h), (i)* or *(j)*, or (5)*(f), (g), (h), (i)* or *(j)* is liable—

(a) in the case of a first conviction, to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment;

(b) in the case of a second conviction, to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment; or

(c) in the case of a third or subsequent conviction, to a fine or to imprisonment for a period not exceeding 15 years or to both such fine

		and imprisonment. (5) Any person who contravenes the provisions of section 17(7), 19A(1), (2), (4)*(a)*, *(b)*, *(c)*, *(d)*, or *(e)*, (5)*(a)*, *(b)*, *(c)*, *(d)* or *(e)* or 20(3) or (4), is liable— *(a)* in the case of a first conviction, to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment; or *(b)* in the case of a second and subsequent conviction, to a fine or to imprisonment for a period not exceeding 15 years or to both such fine and imprisonment. (6) Any person who contravenes the provisions of section 19A(6), is liable— *(a)* in the case of a first conviction, to a fine of R1 000 000 or to imprisonment for a period not exceeding 5 years, or to both such fine and imprisonment; or *(b)* in the case of a second or subsequent conviction, to a fine of R 2000 000 or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment. (7) Any person who contravenes the provisions of section 54(3), is liable, on conviction to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment. (8) Any electronic communications service provider who contravenes the provisions of section 54(4), is liable, on conviction to a fine not exceeding R1 000 000 or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.''.
Act No. 75 of 2008	**Child Justice Act, 2008**	*(a)* The addition of the following **[item]** items to Schedule 2: "**26.** Any offence contemplated in— *(a)* section 2, 3 or 4 of the Cybercrimes Act, 2019; *(b)* section 5, 6, 7 or 11(1) of the Cybercrimes Act, **[2019]** 2020, where the damage caused is below an amount of R5000; *(c)* section 14, 15 or 16 of the Cybercrimes Act, **[2019]** 2020; or *(d)* section 8, 9 or 10 of the Cybercrimes Act, **[2019]** 2020, where the amount involved is below R1500. **27.** An offence contemplated in section 11A(1) and (2) of Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007.". *(b)* The addition of the following **[item]** items to Schedule 3: "**23.** Any offence contemplated in— *(a)* section 5, 6, 7 or 11(1) of the Cybercrimes Act, **[2019]** 2020, where the damage caused **[exceeds]** is an amount

		of R5000 or more; *(b)* section 8, 9 or 10 of the Cybercrimes Act, 2019, where the amount involved **[exceeds]** is R1500 or more; or *(c)* section 11(2) of the Cybercrimes Act, **[2019]** 2020. **24.** An offence contemplated in section 11A(3) of Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007.".