SOUTHERN AFRICA LITIGATION CENTRE

SALC Submission on the Computer Crime and Cybercrime Bill, 2020
13 October 2020

Introduction
We thank Parliament for the opportunity to make these submissions and would like to recommend that the following sections be amended to ensure that they are constitutionally compliant and in line with the principles of legality.

In summary, we propose the following amendments to the Bill:

Section in Bill	**Proposed amendment**
Section 2 - interpretation	Narrow definitions of 'cyber bullying' and 'computer data' and remove the definition 'thing'.
	Change the definition of 'multiple electronic messages' from more than 1 recipient to more than 1000 recipients.
	Delete all definitions linked to offences which are removed from the Bill: 'fake news', 'sexual grooming', 'pornography.
	Define 'critical information infrastructure' in a schedule to the Bill not in subsequent Regulations.
	Define 'court' to refer only to the High Court.
Section 6 – illegal data interference	Define 'unauthorised access' to mean access which is prohibited in terms of the law.
	Delete sections 6(6) and 6(7) and consider deletion of sections 6(2) – 6(5).
Section 7 – data espionage	Limit provision to specific categories of data.
Section 9 – illegal devices	Delete provision.
Section 13 – cyberterrorism	Delete provision.
Section 14 – child pornography	Delete provision.
Section 17 – cyberbullying and cyberstalking	Delete cyberstalking and define cyberbullying.
Section 19 – fake news	Delete provision.

Section 21 and 22 – racist, hate speech and xenophobic material or insult	Define hate speech more broadly.
Section 28 – failure to permit assistance	Delete provision.
Section 29 – harassment	Limit provision to only apply to cases which are severe and repeated. Add a civil remedy of obtaining a restraining order.
Section 30 – intellectual property rights	Delete provision.
Section 32 – extra-territorial jurisdiction	Delete section 32(1)(d).
Section 34 – search and seizure	Instead of referring to 'thing' refer to 'computer system'.
Section 35 – assistance	Narrow provision and delete section 35(1).
Section 36 – production order	Require court to be specific in its order.
Section 37 – expedited preservation of traffic data	Limit period from 28 days to 7 days.
Section 41 – forensic tool	Limit the provision to reduce abuse and provide remedy where abuse has occured.
Section 49 – forfeiture of assets	Amend
Section 50 – general provision on cybercrimes	Delete provision.
All penalties referred to in the Bill.	Reduce the amounts of fines and periods of imprisonment to ensure there are proportionate to the offence.

We note that the Computer Crime and Cybercrime Bill seeks to follow the guidance set by SADC in its Model law on Computer Crime and Cybercrime[1] and the Commonwealth Model law on Computer and Computer Related Crime.[2] Where the Bill exceeds this guidance and has the potential to infringe on freedom of expression, we note those inconsistencies below.

PART 1 - Interpretation – section 2

Some of the definitions in this section are potentially overbroad, including:

[1] International Telecommunication Union Development Bureau (2013).
[2] Commonwealth Secretariat (2017).

- 'computer data' – which refers to "any representation of facts, concepts, information (being either texts, audio, video or images), machine readable code or instructions, in a form suitable for processing in a computer system".
    - Although this definition is the same as in the SADC Model law, the definition remains overly broad in its wording.
- 'cyberbullying' – which refers to the "use of electronic communication to bully a person typically by sending messages of an intimidating or threatening nature".
    - This definition and the offence itself is not included in the SADC Model law and it requires an explanation for its inclusion. As the definition stands, it is quite subjective.
- 'cyberstalking' – which refers to the "use of the internet or other electronic means to inflict repeated unwarranted actions on a natural or juristic person(s), including false accusations, defamation, slander, libel, monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass; which may result in mental or corporate abuse".
    - This definition and the offence itself is not included in the SADC Model law and it requires an explanation for its inclusion. As the definition stands, it is quite subjective.
- 'cyberterrorism' – which refers to deliberate actions using computer systems with the intention to cause serious harm to human lives, way of life, infrastructure or the economy, or to cause fear or terror in a community, nation or group of nations".
    - This definition and the offence itself is not included in the SADC Model law and it requires an explanation for its inclusion. As the definition stands, it is quite subjective and overly broad, particularly phrases such as "way of life".
- 'device' includes but is not limited to – (a) components of computer systems such, (b) storage components and systems, (c) input devices and (d) output devices.
    - This definition is different from the SADC Model law to the extent that subsections (c) and (d) include the phrase "and any other gadget" that can respectively transfer information to or receive information from a computer system.
- 'fake news' refers to a form of "news or statement through any medium including social media with the intention to deceive another person or persons".
    - This definition and the offence itself is not included in the SADC Model law and it requires an explanation for its inclusion. As the definition stands, it is quite subjective and overly broad.
- 'multiple electronic messages' – refers to a mail message including e-mail and instant messaging sent to more than one recipient.

- It is to be noted that the SADC Model law suggests that this should refer to messaging to 'more than 1000' recipients, and of concern that the Bill limits it this number to 'more than 1'. Clearly this definition is overly broad.

- 'pornography' – which is similar to the definition in the Sexual Offences and Domestic Violence Act of 2018, with the difference that it is not restricted to a visual presentation, but refers instead to a "visual, text or audio presentation".
- 'racist, xenophobic and hate speech' – refers to "any material, including but not limited to any image, video, audio recording or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, which may be based on race, colour, descent, national or ethnic origin, religion, creed or social or economic standing, political opinion or disability".
  - Reference to hate speech is not included in the SADC Model law.
  - Hate speech ought to be broadened to include grounds such as sex, gender, sexual orientation and gender identity.
- 'sexual grooming' – refers in the Bill to "intentionally befriending or establishing an emotional connection with a child, or an adult who is legally not able to consent, to train them to agree to participate or lower their inhibitions, in acts of sexual abuse or exploitation".
  - This definition is not included in the SADC Model law.
  - The phrase 'sexual grooming' is not defined in the Sexual Offences and Domestic Violence Act, but the acts involved in the offence is described in Act in some detail. It is accordingly problematic that there is an attempt to define the offence here in a cursory manner.
- 'thing' includes but is not limited to –

  a) A computer system or part of a computer system;
  b) Another computer system, if –
     i. Computer data from that computer system is available to the first computer system being searched; and
     ii. There are reasonable grounds for believing that the computer data sought is stored in the other computer system; or
  c) A computer data storage medium.
     - Although this definition is also included in the SADC Model law, the word 'thing' is likely to lead to misuse.

PART 2 – Offences and Penalties

The penalties outlined in this part, whilst not mandatory, are incredibly high, and if not disproportionate in themselves can foreseeably lead to sentences imposed by courts which are arbitrary and disproportionate. In addition to all the penalties being disproportionately high, the reasons for the differences in penalties for different offences is often unclear, for example:

- Using an illegal device to commit an offence can lead to a fine of E100m or 25 years' imprisonment or both (section 9), even though

the offence being committed might be quite benign. In contrast, committing computer related forgery or computer related fraud can result in a lesser sentence of E10m or 10 years' imprisonment or both (section 10 and 11 respectively), but using a botnet to disrupt a service can attach E100m or 20 years' imprisonment.

- The offences of cybersex or sexual grooming with a child, cyberbullying, cyber stalking, harassment, and trafficking in humans, all attach a penalty of up to E10m fine or 10 years' imprisonment or both. Fake news and violation of intellectual property rights, which do less harm to the individual attach the same penalties of E10m or 10 years' imprisonment.
- Some offences have little congruence between the fine and the number of years in imprisonment: E1m or 15 years' imprisonment (distribution of pornography); E15m or 15 years' imprisonment (racist, hate speech or xenophobic material) versus E10m or 20 years' imprisonment (racist, hate speech or xenophobic motivated insult).

Some of these offences are discussed below:

Illegal data interference – section 6

In terms of section 6(1)(g) and section 6(2), it is an offence to intentionally and without lawful excuse deny access to computer data or services to any person authorised to access it, with a fine up to E10m or 10 years' imprisonment.

Section 6(3) makes it an offence to intentionally and without lawful excuse or justification (b) "access or destroy any computer data, for the purposes of concealing information necessary for an investigation into the commission or otherwise of an offence; or (c) receive computer data that that person is not authorised to receive." Again, the penalty is up to E10m or 10 years' imprisonment or both.

Section 6(6) provides that the penalty increases to up to E100m or 20 years' imprisonment if the data relates to "a critical database" or a database concerned with national security or an essential service. What constitutes a critical database is not defined.

Despite these disproportionately high sentences, section 6(7) provides that "it is immaterial whether an illegal interference or any intended effect, is permanent or temporary".

Importantly, sections 6(2) to 6(7) are not included in the SADC Model law, and ought not to be included in the Bill. Section 6(6) and 6(7) in particular are so overly broad that they can not possibly pass constitutional muster.

Data espionage – section 7

The SADC Model law contains a similar provision, but also notes that a country could choose to limit the espionage to certain categories of data. This approach would be advisable since the offence as it stands now could inhibit whistleblowing and discourage open governance. The penalty on conviction is up to E10m or 10 years' imprisonment or both. It would be hard for an ordinary citizen to know what data is "specially protected against unauthorised access" without at least cross-referencing to other laws in which such data is protected. Without such cross-referencing, "unauthorised access" could be interpreted broadly to include data which is not legally protected from access, but which an official has arbitrarily declared to be prohibited from access. There is also no defence to the offence.

Illegal system interference – section 8
Section 8(2) makes it an offence to intentionally and without lawful excuse or justification seize or destroy any computer storage medium, with a penalty of up to E10m or 10 years' imprisonment or both. There is no corresponding subsection in the SADC Model law, and for good reason, since the subsection is overly broad and can easily lead to abuse.

Hindering or interfering with a computer system that impacts on the operations of critical information infrastructure can result in E100m or 20 years' imprisonment or both, in terms of section 8(3). Critical information infrastructure will be defined in Regulations. In the absence of such definition at the time of enactment of the Bill, this section would be too vague to be lawful.

Illegal devices – section 9
Notably the SADC Model law comments that a country may decide not to make this an offence or to limit the offence to only specific types of devices. The offence, which makes it an offence to use a device to commit an office, in essence results in double criminalisation - criminalising both an offence and the means of carrying out the offence. This is even more of a concern in the light of the penalty imposed for the offence of up to E100m or 25 years' imprisonment. It should also be noted that section 9 was incorrectly copied from the SADC Model law, which results in a different meaning and should be rectified (see subsection (aa)).

Cyberterrorism – section 13
The word 'cyberterrorism' is defined in the Bill to refer to deliberate actions using computer systems with the intention to cause serious harm to human lives, way of life, infrastructure or the economy, or to cause fear or terror in a community, nation or group of nations".

The definition itself is overly broad, and is even broader that the definition of terrorism in the Suppression of Terrorism Act, which definition is itself the subject of litigation before the Supreme Court (see *Thulani Maseko and Others v Prime Minister of Swaziland and Others* [2016] SZHC 180). For example, the phrase "way of life" is simply too subjective for legislative

clarity. Reference to "infrastructure" in the definition is also much broader than a similar reference in the Suppression of Terrorism Act, which refers to "essential infrastructure" (section 2(2)(g) of the STA).

The Bill makes it is an offence to use a computer system to join a known or unknown terrorist group "driven by political ideologies, religion or hate of political systems, with the intention of forcing change or causing fear to general society" (section 13(1)(a)).

The underlined phrases above are vague and overly broad. In the absence of a group having been designated as a terrorist group by the State in terms of the Suppression of Terrorist Act, as amended in 2017, section 13(1)(a) becomes absurd as it could refer to any group anywhere in the world, including one that that accused person him or herself were not aware espouses terrorist beliefs. There are also no defences to the offence nor are there processes or an indication of how a group will be defined as terrorist.

Section 13(c) makes it an offence to promote the interests of such organisations whilst section 13(d) makes it an offence to access websites or information sources of such organisations. Unless an organisation is designated as a terrorist group in terms of a legitimate law, section 13(c) is overly broad in that it could apply to someone promoting those interests of the organisation which are benign or lawful, thus infringing on the right to freedom of expression and association. Section 13(d) is also overly broad as it does not preclude someone simply accessing those websites for research and information purposes, thus infringing on the right to access information.

Doing any of these acts could amount to an offence of cyberterrorism and a conviction of up to E15m or 25 years' imprisonment or both. Given that these offences are overly broad, the penalties attached to them are disproportionate.

Notably, there is no reason to have a specific offence of cyberterrorism outside of the parameters of the Suppression of Terrorism Act, as amended in 2017 and interpreted by the High Court.

Child pornography – section 14

The Bill refines 'pornography' similar to the definition in the Sexual Offences and Domestic Violence Act of 2018, with the difference that it is not restricted to a visual presentation, but refers instead to a "visual, text or audio presentation". Although the offence is also dealt with in the SADC Model law, that is on the assumption that a country might not have a similar offence in other legislation. It does not mean that the SADC Model law suggests a duplication of offences already in existence in other domestic laws. Notably, the SADC Model law also restricts the offence of production of child pornography to it being "for the purpose of distribution on a computer

system", whilst the Bill does not add this qualification, does extending it beyond the reach of the Bill and duplicating what exists in the SODVA. The defence in the Bill of the pornography having been produced for a genuine artistic, educational, public benefit or cultural event, is not included in the SADC Model law.

The Sexual Offences and Domestic Violence Act, 2018, deals extensively with child pornography and imposes a range of sentences for using a child for pornography, making or benefiting from child pornography (up to 25 years' imprisonment); distributing child pornography (up to 20 years' imprisonment); and possessing child pornography (15 years or E75000).

In contrast, section 14(1) of the Bill, places all these offences under one heading where the medium is a computer system and sets a sentence up to 25 years' imprisonment without the option of a fine. There is no reason for duplicating the offence in the Bill since it is covered in relation to computer systems within the definition in the SODVA. To avoid confusion it is suggested that the section be deleted from the Bill.

The Bill refers to 'sexual grooming' as "intentionally befriending or establishing an emotional connection with a child, or an adult who is legally not able to consent, to train them to agree to participate or lower their inhibitions, in acts of sexual abuse or exploitation". This section does not define what "legally not able to consent" means.

Sections 14(4) and 14(5) make it an offence to engage in cybersex or sexual grooming with a child or a person who is not legally capable of consenting, with the penalty or a E10m fine or 10 years' imprisonment or both. Cybersex is not defined in the Bill.

Section 38 of the Sexual Offences and Domestic Violence Act describes the offences of sexual grooming in great detail and attaches an imprisonment of up to 25 years' imprisonment. Creating different and contradictory offences in a law separate from the Sexual Offences and Domestic Violence Act is unnecessary. The Bill also limits the offence and sentence in comparison to how it is referred to in the Sexual Offences and Domestic Violence Act. It is proposed that only one law deals with the offence, and that the SODVA is the appropriate law to do so since it also provides a range of other protective provisions for victims of such offences.

Prohibition of distribution or publication of pornography – section 15

Section 15 is almost a replica of section 23 of the Sexual Offences and Domestic Violence Act, with the exception being in relation to the penalties imposed. Section 15(1) imposes a penalty of E1m or 15 years' imprisonment and section 15(2) imposes a penalty of E1m or 25 years' imprisonment where the offender had parental control over the child. In contrast, section 23(1) of the SODVA imposes a penalty of E50 000 or 15 years' imprisonment and section 23(2) imposes a penalty of E75 000 or 25 years' imprisonment where the offender had parental control over the child. Again the discord

between the Bill and the SODVA is likely to lead to confusion and it is recommended that only one law attends to this, preferably the SODVA.

Cyberbullying and cyberstalking – section 17
Engaging in or abetting cyberbullying attaches a penalty of up to E5m or 5 years' imprisonment, while engaging in or abetting cyberstalking attached a penalty of up to E10m or 10 years' imprisonment.

The Bill defines 'cyberbullying' as the "use of electronic communication to bully a person typically by sending messages of an intimidating or threatening nature".

The Bill defines 'cyberstalking' as the "use of the internet or other electronic means to inflict repeated unwarranted actions on a natural or juristic person(s), including false accusations, defamation, slander, libel, monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass; which may result in mental or corporate abuse".

The offence of cyberbullying is unclear. The Bill attaches a lesser penalty for cyberbullying than for cyberstalking, even though the former could in some instances result in similar or more severe harm. The Bill does not provide a remedy of a restraining order for cases where the cyberbullying is of a nature that does not warrant imprisonment.

The offence of cyberstalking is already provided for under the Sexual Offences and Domestic Violence Act, which in that Act defines unlawful stalking to include stalking by electronic means, and is not limited to acts of a sexual nature. The SODVA also provides a remedy of a restraining order.

Fake news – section 19
Publishing "any statement or fake news through any medium, including social media, with the intention to deceive any other person or group of persons" is an offence and liable on conviction to up to E10m fine of 10 years' imprisonment or both.

'fake news' refers to a form of "news or statement through any medium including social media with the intention to deceive another person or persons".

The offence of fake news is highly subjective and overly broad and ought to be qualified further or repealed altogether. Intentionally deceiving only one person ought never to be an offence under this section, and if the deceit was for a purpose of fraud, for example, that would be the appropriate offence to charge a person with.

Importantly, similar offences have been declared unconstitutional by several regional and domestic courts in Africa.

The ECOWAS Community Court of Justice in February 2018[3] concluded that the offences of sedition, criminal libel and publication of false news were "inacceptable instances of gross violation of free speech and freedom of expression". It emphasised that the right to freedom of expression is "not only the cornerstone of democracy, but indispensable to a thriving civil society" – "wide or vague speech-restricting provisions forces self-censorship". The Court pointed out that these offences originated in an era when freedom of expression was not recognised as a fundamental right.

A similar decision was made by the East African Court of Justice in March 2019, when it concluded that several provisions of Tanzania's Media Services Act No. 120 of 2016 violated freedom of expression, including offences relating to prohibited publications, sedition, criminal defamation and false news.[4]

In Uganda, the Supreme Court declared the false news offence unconstitutional in 2004.[5] The Court examined the offence in the context of the scope and importance of the right to freedom of expression and held that the wording of the offence was vague.

In Zimbabwe, the Supreme Court struck down the offence of false news in 2000.[6] The Court discussed the subjective nature of the concept of "truth." - "Often the line between fact and opinion is blurred. There is a danger that the accepted view becomes confused with the right or correct view." The Court held that because the provision did not require proof of actual negative consequence, merely the likelihood of such a consequence, it was too vague and creates a chilling effect on the practice of journalism.

In Zambia, the High Court declared the false news offence unconstitutional in 2014.[7] The Court recognised the colonial history of the offence, and that the context in which the offence was introduced differed markedly from the present day. The Court highlighted that the existence of the offence can contribute to a culture of fear amongst journalists.

Racist, hate speech or xenophobic material – section 21

Intentionally and without lawful excuse producing, makes available, distributing or transmitting racist, hate speech or xenophobic material

[3] *Federation of African Journalists and Others v Republic of Gambia Judgement* ECW/CCJ/JUD/04/18.
[4] *Media Council of Tanzania and Others v Tanzania*, Ref. No. 2 of 2017, EACJ.
[5] *Obbo and Another v Attorney General* [2004] 1 EA 265 (SCU).
[6] *Chavunduka and Others v Minister of Home Affairs and Another* 2000 (1) ZLR 552.
[7] *Chipenzi v Attorney General* [2014] ZMHC 112.

through a computer system is an offence with a fine of up to E15m or 15 years' imprisonment or both.

'racist, xenophobic and hate speech' – refers to "any material, including but not limited to any image, video, audio recording or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, which may be based on race, colour, descent, national or ethnic origin, religion, creed or social or economic standing, political opinion or disability".

Racist, hate speech and xenophobic motivated insult – section 22
Intentionally and without lawful excuse publicly through a computer system using language that harms the reputation or feelings of persons for reasons that they belong to a group distinguishable by race, colour, descent or national or ethnic origin as well as religion, constitutes an offence. The penalty is up to E10m or 20 years' imprisonment or both.

It is interesting to note that the SADC Model law uses the stronger word of "insults" instead of the phrase "harms the reputation or feelings".

In the case of both sections 21 and 22, we submit that by including the term "hate speech", the description of groups ought to be broadened to other groups against whom hate speech is committed, including on the basis of sex, gender, sexual orientation, and gender identity.

Disclosure of details of investigation – section 27
A service provider who receives a confidential order related to a criminal offence commits an offence if information relating to the order or anything done under the order is intentionally and without lawful excuse disclosed. The penalty is E1m or 3 years' imprisonment.

Failing to assist someone based on an order also constitutes and offence with similar penalty (section 28). Notably, the SADC Model law suggests that a country can decide to not criminalise failure to assist where other remedies are available.

Harassment utilising means of electronic communication – section 29
Intentionally and without lawful excuse initiating "any electronic communication, with the intention to coerce, intimidate, insult, harass, or cause emotional distress to a person using a computer system, to support hostile behaviour" is an offence. The penalty is up to E10m or 10 year' imprisonment or both.

The offence of harassment is much broader than what is proposed in the SADC Model law. The Model law does not include "insult" under this offence and limits the offence to instances which are "severe, repeated **and** hostile", not simply "hostile". We submit that the approach of the SADC Model law is

much clearer and preferred. We are concerned that the offence could be used to persecute human rights defenders.

Violation of intellectual property rights – section 30
Using a computer or electronic device to violate intellectual property rights constitutes an offence with a penalty of up to E10m or 10 years' imprisonment or both. The issue of intellectual property rights is not addressed in the SADC Model law and need also not be addressed here since it is adequately catered for in laws specifically relating to intellectual property rights.

Extra territorial jurisdiction – section 32
The Act is applicable also to offences committed outside Eswatini "with a direct impact to the Kingdom of Eswatini" (section 32(1)(d)). Section 32(1)(d) is not in the SADC Model law ought to be removed. The subsection is overly broad in the use of the term "direct impact" and is likely to be used to curtail freedom of expression and external criticism of the State.

Search and seizure – section 34
The Bill defines a court to refer to a magistrates' court or High Court. This is likely to cause problems in interpretation. Given the complexity of the matters in the Bill, it is proposed that the Bill refer to the High Court only.

A court can issue a warrant of "there may be in a place a thing or computer data" which "may be material as evidence in proving an offence".

The Bill defines the term 'thing' to include but is not limited to –

a) A computer system or part of a computer system;
b) Another computer system, if –
    i. Computer data from that computer system is available to the first computer system being searched; and
    ii. There are reasonable grounds for believing that the computer data sought is stored in the other computer system; or
c) A computer data storage medium.

The offence and definition of thing is likely to provide law enforcement agents with a wide scope to seize equipment as part of a fishing expedition instead of with a specific offence in mind. The provision can be used to target persons who are critical of the State.

Assistance – section 35
Where a court ordered a warrant, the person enforcing the warrant may be assisted as necessary by any person with knowledge about the computer system. In terms of section 35(2) however, a person who is requested to so assist to provide information, to access the computer, to copy the computer data, etc, shall assist if reasonably required and requested by the person authorised to make the search. To the extent that this provision can be used

to intimidate persons to disclose passwords and thus to risk incriminating themselves, this offence could infringe on fair trial rights.

Production order – section 36
A court can order that a service provider produces information about persons who subscribe to the service. It is submitted that there should be limitations to what information a service provider may disclose and the court order ought to require specific information relating to a specific offence as opposed to a generalised order.

Expedited preservation of traffic data – section 37
The Bill states that 'traffic data' is generated by a computer system as part of the chain of electronic communication and includes information such as the communication's origin, destination, route, time, date, size, duration etc. A law enforcement officer can give written notice to someone in control of computer data to preserve the data for 28 days for the purposes of a criminal investigation. If additional time is required for the investigation a court order is required and the period can then only be extended by a further 28 days.

This provision is of great concern since it far exceeds what is proposed by the SADC Model law, which is that the data only be preserved for 7 days and on court order for a further 7 days. It would be unreasonable for a law enforcement officer to have the power to order preservation of data for 28 days in the absence of a court order.

Partial disclosure of traffic data – section 38
A law enforcement officer can through written notice require disclosure of relevant traffic data about a specified communication to identify the service provider or path through which it was transmitted. Again, allowing a law enforcement officer to obtain information without a warrant is a deviation from acceptable criminal procedure.

Forfeiture of assets – section 49
Conviction under the Act can result, among other things, to forfeiture or one's travelling document until the fine has been paid or sentenced served. Given the high fines set in this Act, the forfeiture of travel documents is a concern, although section 49(3) does allow a person to apply for the travel documents if the travel is for the purpose of medical treatment and it is in the interest of the public.

General provision on cybercrimes – section 50
The Bill provides that "except as provided for in this Act, any offence under any Act which is committed in whole or in part through the use of a computer electronic device or in electronic form is deemed to have been made under that Act and the provision of that Act shall apply with the necessary modifications to the person who commits the offence." In the light

of this provision, there is basically no reason to include provisions already covered in the Sexual Offences and Domestic Violence Act.