ARTICLE 19

Kenya: Cybercrime and Computer Related Crimes Bill

Legal analysis

Executive summary

In July 2014, ARTICLE 19 analysed the first draft of the Cybercrime and Computer related Crimes Bill in Kenya ('Cybercrime Bill'). In particular, we examined the compatibility of the Bill against international and comparative standards for the protection of freedom of expression and the right to privacy.

The Cybercrime Bill is an initiative of the Office of the Director of Public Prosecutions (ODPP). It seeks to equip law enforcement agencies with the necessary legal and forensic tools to tackle cybercrime, which is said to have cost nearly KES 2 billion (USD 23 million) to the Kenyan economy in 2013. The Bill comes on the heels of a Cyber Security conference in June 2014 where the Telecommunications Service Providers Association of Kenya (TESPOK) and cyber security groups from Canada, Singapore, South Africa, India and USA discussed the role of the private sector in tackling cybercrime. The meeting recommended the adoption of a comprehensive cybercrime law in light of the perceived failings the existing legal framework in dealing with recent terrorist attacks.

Our analysis shows that the provisions dealing with 'content-related' offences in the draft Cybercrime Bill fall well below international standards on freedom of expression. In particular, the Bill provides for incredibly broad speech offences that could have a devastating effect for freedom of expression online in Kenya. It also provides for unduly broad offences against computers and other computer-related offences. By contrast, we conclude that the procedural safeguards to investigate and prosecute cybercrimes are generally adequate. Nonetheless, we offer recommendations in order to further improve them in line with international standards on freedom of expression and privacy.

Key Recommendations

- The definition of computer system should closely follow the definition contained in the Cybercrime Convention. In particular, the definition of computer system should make explicit reference to 'automatic processing of data';
- In the definition of 'damage', the word 'serious' should be inserted between 'any' and 'impairment' and between 'any' and 'loss';
- The words 'threatens public health or public safety' should be removed from the definition of 'damage' and replaced, if appropriate, with a more targeted definition of the kind of damage sought to be addressed by the computer offences contained in the Bill;
- A definition of 'service provider' should be added consistent with the equivalent definition contained in the Cybercrime Convention.
- Section 3 should be rephrased to criminalise the unauthorised access to computer data by infringing security measures with intent to obtain computer data or other dishonest intent.
- The reference to 'any' law in section 4 (1) should be removed and replaced with both specific and serious offences.
- Section 5 should introduce a requirement that the unauthorised modification of computer should cause serious harm to computer data or other particular interest in line with the recommendations of the Cybercrime Convention.
- Section 7 should be removed;
- In section 9, 'knowingly' should be replaced with 'intentionally';
- Section 9 should follow more closely the definition of 'system interference' under Article 5 of the Cybercrime convention in order the simplify the language of that section;

- Section 9 should include a requirement that any such interference must 'seriously' hinder the functioning of a computer system.
- 'Knowingly' should be replaced by 'intentionally' in section 10 (1).
- Section 11 should be entirely struck out.
- 'Protected systems' should be defined in the Bill along the lines of the definition contained in the US Computer Fraud and Abuse Act. Short of such clarification, serious consideration should be given to removing section 14 entirely.
- Section 16 as currently drafted should be struck out in its entirety. We recommend that the drafters of the Bill should refer to the COE Cybercrime Convention or the definition of child pornography laid down in the African Union Convention on Cyber Security and Personal Data Protection.
- Section 17 of the Bill concerning hate speech online should be struck out in its entirety.
- Section 18 of the Bill should be struck out in its entirety. Legislation against stalking and harassment should be dealt with by way of the general criminal law, rather than in the context of cybercrime.
- Section 35 (f), which deals with the extra-territorial application of Kenyan law to places where any result of the offence has an effect in Kenya, should be removed.
- Section 40, which introduces a general penalty, should be removed.

Table of Contents

Introduction

In July 2014, ARTICLE 19 analysed the first draft of the Cybercrime and Computer related Crimes Bill in Kenya (Draft Bill or Bill). In particular, we examined the compatibility of the Bill against international and comparative standards for the protection of freedom of expression and the right to privacy.

The Draft Bill is an initiative of the Office of the Director of Public Prosecutions (ODPP). It seeks to equip law enforcement agencies with the necessary legal and forensic tools to tackle cybercrime, which is said to have cost nearly KES 2 billion (USD 23 million) to the Kenyan economy in 2013.[1] The Bill comes on the heels of a Cyber Security conference in June 2014 where the Telecommunications Service Providers Association of Kenya (TESPOK) and cyber security groups from Canada, Singapore, South Africa, India and USA discussed the role of the private sector in tackling cybercrime.[2] The meeting recommended the adoption of a comprehensive cybercrime law in light of the perceived failings the existing legal framework in dealing with recent terrorist attacks.[3]

ARTICLE 19 notes that the Draft Bill is still in its early stages. With this analysis, we hope to contribute our extensive experience of both working on freedom of expression issues in Kenya and working on issues related to protection of freedom of expression online. In particular, we have analysed various Cybercrime Laws around the world, including in Brazil,[4] Iran[5], Pakistan[6] and Cambodia.[7] Therefore, we believe that we are particularly well placed to assess the Bill, which forms part of the legal framework governing freedom of expression on the Internet in the country.

Our analysis shows that the provisions dealing with 'content-related' offences in the Draft Bill fall well below international standards on freedom of expression. In particular:

- it provides for incredibly broad speech offences that could have a devastating effect for freedom of expression online in Kenya.
- It provides for unduly broad offences against computers and other computer-related offences. By contrast, we conclude that the procedural safeguards to investigate and prosecute cybercrimes are generally adequate.

Nonetheless, we offer recommendations in order to further improve them in line with international standards on freedom of expression and privacy. We also explain the ways in which the more problematic provisions in the Bill could be made compatible with international standards for the protection of freedom of expression and privacy. We set out our key recommendations at the end of each section.

[1] IT Web Africa, Cybercrime to cost Kenya almost 23 USD million in 2013, 27 November 2013.
[2] Coastweek, Cyber experts to assess Kenya's Readiness to Combat Cybercrime.
[3] All Africa, ICT Ministry Draws Strategies to Curb Cyber Crime, 12 June 2014.
[4] ARTICLE 19, analysis of the Draft Cybercrime Law of Brazil, January 2012.
[5] ARTICLE 19, analysis of the Computer Crimes Law of the Islamic Republic of Iran, January 2012.
[6] ARTICLE 19, analysis of Pakistan Telecommunications (Re-organisation) Act, 1996, January 2012.
[7] ARTICLE 19, Secret Draft Cybercrime Law Seeks to Undermine Free Speech Online, April 2014.

International standards

The protection of freedom of expression under international law

The right to freedom of expression is protected by a number of international human rights instruments that bind states, including Kenya, in particular Article 19 of the **Universal Declaration of Human Rights** (UDHR) [8] and Article 19 of the **International Covenant on Civil and Political Rights** (ICCPR).[9]

Kenya also ratified the 1983 **African Charter on Human and Peoples' Rights** (ACHPR) which guarantees the right to freedom of expression in Article 9.[10] Additional guarantees to freedom of expression are provided in the 2002 **Declaration of Principles on Freedom of Expression in Africa** (African Declaration) in Article II.[11]

Additionally, **General Comment No 34**,[12] adopted by the UN Human Rights Committee in September 2011, explicitly recognises that Article 19 ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[13] In other words, the protection of freedom of expression applies online in the same way as it applies offline. State parties to the ICCPR are also required to consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[14] The legal framework regulating the mass media should take into account the differences between the print and broadcast media and the Internet, while also noting the ways in which media converge.[15]

Similarly, the four special mandates for the protection of freedom of expression, including the African Special Rapporteur on Freedom of Expression and Access to Information, have highlighted in their **Joint Declaration on Freedom of Expression and the Internet** of June 2011 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[16] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary. They also promote the use of self-regulation as an effective tool in redressing harmful speech.

As a state party to the ICCPR, Kenya must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 ICCPR as interpreted by the UN Human Rights Committee and that they are in line with the special mandates' recommendations.

[8] *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit)
[9] Article 2 of the ICCPR, GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[10] Kenya ratified the African Charter on Human and Peoples' Rights on 23 January 1992.
[11] Adopted at the 32nd Session of the African Commission on Human and Peoples' Rights, 17-23 October 2002.
[12] CCPR/C/GC/3, adopted on 12 September 2011.
[13] *Ibid*, para. 12.
[14] *Ibid*., para. 17.
[15] *Ibid*., para. 39.
[16] See Joint Declaration on Freedom of Expression and the Internet, June 2011.

Limitations on the Right to Freedom of Expression

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms. Restrictions on the right to freedom of expression must be strictly and narrowly tailored and may not put in jeopardy the right itself. The determination whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must:

- **prescribed by law**: this means that a norm must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[17] Ambiguous, vague or overly broad restrictions on freedom of expression are therefore impermissible;

- **pursue a legitimate aim**, exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR as respect of the rights or reputations of others, protection of national security, public order, public health or morals. As such, it would be impermissible to prohibit expression or information solely on the basis that they cast a critical view of the government or the political social system espoused by the government;

- should be **necessary to secure the legitimate aim and meet the test of proportionality**. Necessity requires that there must be a pressing social need for the restriction. The party invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific and individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result. [18]

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[19]

Online content regulation

The above principles have been endorsed and further explained by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, in two reports in 2011.[20]

In September 2011 report, the Special Rapporteur also clarified the scope of legitimate restrictions on different types of expression online.[21] He also identified three different types of expression for the purposes of online regulation:

- expression that constitutes an offence under international law and can be prosecuted criminally;
- expression that is not criminally punishable but may justify a restriction and a civil suit; and
- expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[22]

[17] *Leonardus J.M. de Groot v. The Netherlands*, No. 578/1994, U.N. Doc. CCPR/C/54/D/578/1994 (1995).
[18] *Velichkin v. Belarus*, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).
[19] General Comment 34, *op.cit.*, para 43.
[20] Report of the UN Special Rapporteur on Freedom of Expression, A17/27, 17 May 2011 and Report of the UN Special Rapporteur on Freedom of Expression, A/66/290, 10 August 2011
[21] *Ibid.*, para.18.
[22] *Ibid.*

In particular, the Special Rapporteur clarified that the only exceptional types of expression that States are required to prohibit under international law are: (a) child pornography; (b) direct and public incitement to commit genocide; (c) hate speech; and (d) incitement to terrorism. He further made clear that even legislation criminalizing these types of expression must be sufficiently precise, and there must be adequate and effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body. [23] In other words, these laws must also comply with the three-part test outlined above. For example, legislation prohibiting the dissemination of child pornography over the Internet through the use of blocking and filtering technologies is not immune from those requirements.

Role of Internet intermediaries and intermediary liability

Special mandates also commented on the role and measures available to intermediaries to censor the content. In particular, the UN Special Rapporteur on freedom of expression also commented on role of intermediaries noted:[24]

> 42. [W]hile a notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown. Moreover, **given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by overcensoring potentially illegal content**. Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences. (Emphasis added)

Accordingly, the four special rapporteurs on freedom of expression recommended in their 2011 Joint Declaration on Freedom of Expression and the Internet that:

> (i) No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information;
> (ii) Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;
> (iii) ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown. [25]

Surveillance of communications

Guaranteeing the right to privacy in online communications is essential for ensuring that individuals have the confidence to freely exercise their right to freedom of expression. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

The right of private communications is strongly protected in international law through Article 17 of the ICCPR,[26] that *inter alia*, state that no one shall be subjected to arbitrary or unlawful

[23] *Ibid,* para. 22
[24] UN Special Rapporteur on Freedom of Expression report, *op.cit*, para. 42.
[25] The 2011 Joint Declaration, *op.cit.*

interference with his privacy, family or correspondence. In General Comment no. 16 on the right to privacy, the UN Human Rights Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives the ICCPR. It also further stated that:

> 8. Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.

The UN Special Rapporteur on promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test: [27]

> [A]rticle 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17.

The Special Rapporteur further defined the scope of legitimate restrictions on the right to privacy as follows: [28]

> States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing there must be "on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.

The lack of ability of individuals to communicate privately substantially affects their freedom of expression rights.[29] For example, the UN Special Rapporteur on Freedom of Expression observed that:

> 59. [T]he right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of administration of criminal justice, prevention of crime or combating terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the

[26] Article 17 states: 1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2) Everyone has the right to the protection of the law against such interference or attacks.
[27] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009.
[28] *Ibid.*, para. 21
[29] C.f. Report of the UN Special Rapporteur on Freedom of Opinion and Expression, 16 May 2011, *op.cit.*

> judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.

He also recommended that States should ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems.[30]

Cybercrime

The Council of Europe Convention on Cybercrime CETS (Cybercrime Convention) is the only binding international instrument in this area.[31] It was adopted in 2001 and has been ratified by 42 countries, including the United States, Australia and Panama, and signed by another 11 countries. The Convention provides helpful guidance on how to draft cybercrime legislation in accordance with human rights standards. In particular, it contains basic definitions, including a definition of computer data, computer system, traffic data and service provider.

The Convention further requires its signatory parties to create offences against the confidentiality, integrity and availability of computer systems and computer data, computer-related offences such as forgery and content-related offences such as the criminalisation of child pornography. In addition, the Convention mandates the adoption of a number of procedural measures to investigate and prosecute cybercrimes, including preservation orders, production orders and search and seizure of computer data.

Finally, and importantly, the Convention makes clear that the above measures must respect the conditions and safeguards for the protection of human rights consistent with the Contracting parties' obligations under the European Convention on Human Rights and the ICCPR.

[30] *Ibid.*, para 84.
[31] The Council of Europe Convention on Cybercrime, CETS No. 185.

Analysis of the Draft Bill

Definitions

Part I of the Draft Bill contains several important definitions, including "access", "computer", "computer service", "computer system", "damage", "data", "intercept in relation to a function of a computer", "modification", "computer programme and "traffic data".

ARTICLE 19 generally welcomes this part of the Bill, which contains overall satisfactory definitions of key terms connected to the prosecution of computer-related crimes. In particular, we note that the definition of traffic data is consistent with the definition contained in the Cybercrime Convention. Nonetheless, we note that the definition of some key terms could be further improved, including the following:

- *Computer system*: while this definition does not appear intrinsically problematic, we note that it fails to include a reference to 'automatic processing of data', which is a key component of the definition of computer systems in the Cybercrime Convention. It is true that other definitions contained in the Bill make reference to 'data processing'. However, we believe that the definition of 'computer system' should make it clear that data processing in this context is 'automatic'.

- *Damage*: the Bill defines damage as including, among other things, 'any' impairment to a computer or the integrity or availability of data, programme, system or information that causes 'any' loss or 'threatens public health or public safety'. We are concerned that this definition of damage is overly broad and would catch minor disruptions or losses to information systems. In our view, the definition of damage for the purposes of cybercrime legislation should reflect the fact that only 'serious' impairment or losses should attract criminal sanctions. Similarly, we believe that the reference to an undefined 'threat' to 'public health' or 'public safety' is unduly broad. Accordingly, we recommend that the definition of 'damage' should be narrowed along the lines suggested in our recommendations further below.

In addition, we note that the Draft Bill fails to provide for a definition of "service provider." Accordingly, we recommend that the Bill include such definition consistent with the definition contained in the Cybercrime Convention.

Recommendation:

- The definition of computer system should closely follow the definition contained in the Cybercrime Convention. In particular, the definition of computer system should make explicit reference to 'automatic processing of data';
- In the definition of 'damage', the word 'serious' should be inserted between 'any' and 'impairment' and between 'any' and 'loss';
- The words 'threatens public health or public safety' should be removed from the definition of 'damage' and replaced, if appropriate, with a more targeted definition of the kind of damage sought to be addressed by the computer offences contained in the Bill;
- A definition of 'service provider' should be added consistent with the equivalent definition contained in the Cybercrime Convention.

Offences against the confidentiality, integrity and availability of computer data and systems

Part II of the Draft Bill creates nine separate offences against the confidentiality, integrity and availability of computer data and systems. These include unauthorised access to computer data, access with intent to commit offences, unauthorised modification of computer data, unauthorised access to and interception of computer service, damaging or denying access to computer system, unauthorised disclosure of access code, system interference, misuse of devices and unauthorised receiving or giving access to a computer programme or data.

General comments

Before laying down our specific concerns relating to some of the above offences, ARTICLE 19 would like to make two general comments.

- *First*, we note that the Bill introduces an unusually high number of computer-related offences. We note, by contrast, that the Cybercrime Convention contains only five such offences whilst the UK Computer Misuse Act 1990 contains four such offences. We have not heard any suggestion, however, that the UK is not properly equipped to deal with 'cybercrime'. We therefore question at the outset the necessity of enacting so many different offences. In our view, and as detailed further below, several all the offences provided for under the Bill could be either regrouped and simplified or entirely removed.

- *Secondly,* we are concerned that the offences contained in Part II of the Bill provide for unduly harsh sentences, from two to three years imprisonment. We respectfully draw attention to the equivalent offences under the UK statute mentioned above, which provide for sentences of imprisonment not exceeding 12 months. We would therefore recommend that the sentences available for offences against the confidentiality, integrity and availability of computer data and systems should be reduced to one-year maximum.

Unauthorised access to computer data

Section 3 of the Draft Bill criminalises anyone 'who causes a computer system to perform a function, knowing that the access they intend to secure is unauthorised'.

ARTICLE 19 considers that the wording of this offence is unduly vague as it fails to explicitly require an infringement of security measures in order for the *actus reus* to be made out as recommended in Article 2 of the Cybercrime Convention. Moreover, the only intent required is that of 'unauthorised access' rather than 'obtaining computer data' or other dishonest intent. For instance, accessing computer data without authorisation for the purposes of testing whether the data kept in a computer system is stored securely could inadvertently become criminalised.

Recommendation:

- Section 3 of the Draft Bill should be rephrased to criminalise the unauthorised access to computer data by infringing security measures with intent to obtain computer data or other dishonest intent.

Access with intent to commit offences

Section 4(1) of the Draft Bill criminalises access to computer systems with intent to commit an offence under 'any' law. Section 4(2) specifies that 'access' for the purposes of sub-section (1) is authorised or unauthorised. ARTICLE 19 has two main concerns in relation to this offence:

- *Lack of legal certainty*: ARTICLE 19 believes that this section is unduly broadly drafted. In particular, the reference to intent to commit an offence under 'any' law fails to comply with the requirements of legal certainty under international law. The criminal law should only criminalise intent to commit both specific and serious offences rather than broadly refer to every possible offence under the sun, however minor. Moreover, the reference to 'any' law fails to establish a rational connection between the access to computer data or programmes and the commission of the further offence.

  Accordingly, we recommend that the offence created by section 4(1) should be significantly narrowed. In particular, it should be made clear that unauthorised access serves as the means to or preparatory act to the commission of a further offence, which should be clearly defined.

  We further note that section 4 in its current form would allow the prosecution of potential whistleblowers in breach of international standards of freedom of expression. Indeed, it would suffice that an individual who is authorised to have access to certain types of computer data and programmes 'intends' to commit an offence under any law, without actually having committed the offence itself (which, as noted above is undefined). For instance, individuals who are authorised to have access to classified material, like Mr Snowden, and who merely 'intend' to release that material could be prosecuted even before they release the material in question. In our view, this perfectly illustrates why section 4 in its current form is overly broad and should make explicit reference to the further offence, which is being targeted.

- *Questionable necessity for the offence:* More generally, we question whether the section 4 offence is necessary given that unauthorised access to computer data is criminalised under the Bill and that most substantive offences that may be committed by means of such unauthorised access, such as bank robbery, would presumably already be covered under the Kenyan criminal code or relevant statute.

Recommendation:

- The reference to 'any' law in section 4 (1) should be removed and replaced with both specific and serious offences.

Unauthorised modification of computer data

Section 5 of the Bill criminalises the unauthorised modification of computer data. ARTICLE 19 notes with concern however that there is no requirement under section 5 that such modification should cause *serious* harm or damage to a particular interest or computer systems. Similarly, the requirement of intent is currently linked to the mere act of modification under section 5 (1) (a) rather than intent to cause serious harm or damage under section 5 (2).

We are concerned that section 5 in its current form would therefore allow individuals to be prosecuted even for minor modifications that only marginally impair the operation of computer systems or other interest in the absence of dishonest or malicious intent.

Recommendation:

- Section 5 should introduce a requirement that the unauthorised modification of computer should cause serious harm to computer data or other particular interest in line with the recommendations of the Cybercrime Convention.

Damaging or denying access to computer system & system interference

Section 7 of the Draft Bill criminalises damage or denial of access to or impairment of a computer system without lawful authority or lawful excuse. It is irrelevant for the purposes of section 7 (2) whether damage or other intended effect is permanent or temporary.

Section 9, meanwhile, punishes anyone who, knowingly and without authority or lawful excuse, interferes with or interrupts or obstructs the lawful use of a computer or impedes or prevents access to or impairs the usefulness or effectiveness of any programme or data stored in a computer.

Both offences carry a prison sentence of 3 years or a fine of up to 5 million shillings in the case of an offence under section 7 or up to 250,000 shillings in the case of an offence under section 9.

Our concerns in relation to the above offences are two-fold:

- *Streamlining the offence of system interference:* ARTICLE 19 queries the usefulness of creating two separate offences that are both ostensibly aimed at dealing with system interference. It is equally unclear to us why the offence under section 7 is punishable with a fine, which is significantly higher than the fine available under section 9, especially given that the extent of the damage does not appear to be a consideration for the purposes of section 7. In our view, section 7 is redundant and should be removed.

- *Proof of serious harm and mens rea:* In any event, both section 7 and section 9 are problematic in that the offence is committed even in the absence of *serious* damage or impairment to a computer system. Moreover, both section 7 and 9 criminalise the inadvertent – rather than wilful - interference with a computer system. Indeed, section 7 does not require any particular mental state whilst section 9 only makes reference to 'knowingly' interfering with a computer. ARTICLE 19 therefore recommends that section 9 - and section 7 if contrary to our recommendation above this section is not removed - should replace 'knowingly' with 'intentionally'.

Recommendation:

- Section 7 should be removed in its entirety;
- In section 9, 'knowingly' should be replaced with 'intentionally';
- Section 9 should follow more closely the definition of 'system interference' under Article 5 of the Cybercrime convention in order the simplify the language of that section;
- Section 9 should include a requirement that any such interference must 'seriously' hinder the functioning of a computer system.

Unauthorised receiving or giving access to a computer program or data

Section 11 (1) criminalises anyone who receives or is given access to any programme or data held in a computer and who is not authorised to receive or have access to that programme or data. It is immaterial for the purpose of the offence whether the person giving the programme or data is has obtained such programme or data with or without authorisation.

In addition, section 11(2) criminalises anyone who is authorised to get access to a programme or data to receive such programme or data from another person in the knowledge that that person is not authorised to get access to that programme or data.

ARTICLE 19 is deeply concerned by this offence, which, in our view, is both arbitrary and incredibly vague:

- To begin with, section 11 (1) would potentially criminalise individuals merely for receiving a computer file or programme despite the fact that the file or programme may not have been solicited and that in the vast majority of cases, it would be impossible for people to know whether or not they are authorised to have access to that file or programme without opening it in the first place. Moreover, the offence would be committed regardless of how sensitive the computer data or file is.

- Secondly, and in any event, we find the purpose of this offence entirely unclear. As such, it is an unjustified restriction on the right to receive information under international human rights law.

- Finally, in our view, the logic of section 11 (2) is fatally flawed. There is little sense in criminalising an individual who is authorised to access a particular computer programme or data for receiving that same programme or data from another who does not have such access. It is again entirely unclear what the purpose of this sub-section is and in our view, it should be entirely removed.

Recommendation:

- Section 11 should be entirely struck out.

Illegal devices or data

Section 10(1) criminalise anyone who knowingly manufactures, sells, procures, imports or distributes devices which are primarily designed for the purpose of committing an offence under sections 1 to 9 of the Bill. Moreover, section 10 (2) of the Bill criminalises anyone who knowingly receives or is in possession of such devices without sufficient excuse or justification.

ARTICLE 19 is concerned that this provision may be used to prosecute individuals or companies producing, distributing, selling or otherwise circulating software used to break Digital Management Rights systems. DRM systems are a type of technology principally used by hardware manufacturers, publishers and copyright holders to control how digital content may be used after sale. DRM systems are controversial from a freedom of expression perspective, as the legitimacy of copyright holders exercising in perpetuity absolute control over the sharing of information is strongly contested. For example, DRM systems prevent individuals from engaging in trivial and non-commercial acts of copyright infringement such as transferring data between their own electronic devices; they can also prevent individuals from using copyrighted works in a way that is ordinarily protected by the defence of "fair use."

Specifically, we are concerned that the *mens rea* for the purpose of section 10 (1) is 'knowledge' rather than 'intent'. Most companies would know that the software they manufacture or sell could be used for dual purposes, including for the purposes of unauthorised access to computer data and systems. Indeed, it is in the nature of technology that it can be used both for legitimate and illegitimate purposes. We believe, therefore, that a higher standard of intent should be introduced so that 'knowingly' in section 10 (1) is replaced with 'intentionally'.

We do appreciate, however, the apparent efforts of the drafters not to criminalise the everyday use of Internet users who seek to remove DRM protections in order to view or listen to a CD or DVD. In this regard, we note that section 10 (2) does provide for the possible exoneration of anyone found in possession of software, which may be used for the purpose of committing an offence under sections 1 to 9 of the Bill, if they can demonstrate a 'sufficient excuse or justification'.

Recommendation:

- 'Knowingly' should be replaced by 'intentionally' in section 10 (1).

Computer-related offences

Part III of the Bill provides for three further computer-related offences, namely 'computer-related forgery' (section 12), 'computer-related fraud' (section 13) and 'unauthorised access to protected systems' (section 14).

The first two offences are consistent with the Cybercrime Convention. At the same time, we note that they involve the use of a computer in order to engage in conduct, which is normally already criminalised offline, namely forgery and fraud. We would therefore encourage the Kenyan government to ensure consistency with existing laws covering this type of criminal conduct so as to avoid unnecessary duplication.

ARTICLE 19 is more concerned by the offence of 'unauthorised access to protected systems'. We note at the outset that 'protected systems' is undefined in the Bill. In the absence of a clear definition, we are concerned that 'protected system' could be interpreted to include devices with DRM protections. This would be worrying for the reasons outlined above, namely that it would criminalise Internet users for largely innocuous and non-commercial acts of copyright infringement.

If 'protected systems' is merely intended to cover more specific computer systems that are used in the context of commercial transactions - as the language of section 14 seems to suggest - that should be made clear. In this regard, we note that under US law, the term 'protected computer' is a statutory term of art which is defined in the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e)(2), as covering both computers used in connection with domestic or foreign commerce and those used by the federal government and financial institutions.[32] In the absence of such clarification in the Bill, in our view, the offence under section 14 seems redundant at best and potentially damaging for freedom of expression at worst.

Recommendations:

- 'Protected systems' should be defined in the Bill along the lines of the definition contained in the US Computer Fraud and Abuse Act. Short of such clarification, serious consideration should be given to removing section 14 entirely.

Content-related offences

ARTICLE 19 is deeply concerned by sections 16, 17 and 19 of the Draft Bill, which deal with "child pornography," "hate speech" and cyber-stalking respectively. In our view, these offences are incredibly broadly drafted and fail to comply with the requirement of legal certainty under international human rights law. We explain our specific concerns in relation to each of these offences further below.

"Child pornography"

Whilst the title of section 16 suggests that the provision deals with child pornography, in reality, it criminalises pornography. In particular, the main test used throughout section 16 is 'obscenity',

[32] See, US Department of Justice, *Prosecuting Computer Crimes,* available at: http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

which is defined by reference to 'laviscious' material or material that appeals to the 'prurient interest' or tends to 'deprave' or 'corrupt' the persons who have access to it. ARTICLE 19 has long fought against obscenity laws, which are based on eminently subjective definitions and rely on the 'gut-feeling' instincts of the government of the day.

Moreover, we note that pornography is not one of the types of expression that must be prohibited under international law. In this regard, the UN Human Rights Committee recently restated that restrictions on freedom of expression for the protection of public morals must be based on a broad understanding of what 'public morals' means, i.e. one that does not derive exclusively from one social, philosophical or religious tradition.

For all these reason, we believe that section 16 represents an unjustified restriction on freedom of expression and would recommend that it should be struck out. At the same time, consistent with the recommendations of the UN Special Rapporteur on freedom of expression and the Cybercrime Convention, we fully agree that child pornography online should be criminalised. In this regard, we draw attention to Article 9 of Cybercrime Convention which lays down a commonly agree definition of offences related child pornography. In the alternative, we would recommend using the definition of child pornography in Article 1 of the African Union Convention on Cyber Security and Personal Data Protection.

Recommendation:

- Section 16 as currently drafted should be struck out in its entirety. We recommend that the drafters of the Bill should refer to the COE Cybercrime Convention or the definition of child pornography laid down in the African Union Convention on Cyber Security and Personal Data Protection.

"Hate speech"

In recent years, ARTICLE 19 has expressed concern that Kenya's existing legislation on "hate speech" went beyond what is required under international human rights law and had the potential effect of restricting legitimate forms of expression. We note that hate speech is already the subject of numerous legislative provisions in Kenya, including section 33(2) of the 2010 Constitution, section 138 of the Penal Code and sections 13 and 62 of the National Cohesion and Integration Act 2008, as well as more general regulation in the context of broadcasting (see e.g. the Kenya Information Communications (Amendment) Act (2013).

It is therefore highly unclear why it should be thought necessary to include in section 17 a separate offence of hate speech in the context of Cybercrime legislation. In our view, to the extent that this provision differs from existing legislation against hate speech, it undermines the principle of equality before the law because it treats individuals committing the same offence differently by reference to whether or not they used a computer. Given the ubiquity of electronic communications in the modern age, we do not consider that this can sensibly be treated as an aggravating factor of any sort. To the extent that hate speech online falls outside the scope of existing hate speech legislation (something which remains unclear), it would be better to address this issue by way of amending the existing legislation rather than create a separate, unnecessary online offence. We therefore recommend that section 17 be removed from the Bill.

Recommendation:

- Section 17 of the Bill should be struck out in its entirety.

Cyber-stalking

The right to privacy requires that the criminal law protect individuals from harassment, threats and other forms of intimidation. To the extent that Kenyan law fails to provide sufficient protection in this area, it is incumbent that the legislature takes immediate steps to ensure that the criminal law is adequate and fit for purpose.

ARTICLE 19 is concerned, however, that section 18 represents an unduly narrow attempt to address problems related to stalking and harassment, while at the same time providing insufficient safeguards against misuse - particularly in the context of legitimate protests and investigative journalism.

- First, it remains unclear why the scope of section 19 should be limited to using "a computer system" (which is defined to include any electronic communication) to harass, intimidate or cause substantial emotional distress or anxiety to another person. It is apparent that such conduct would be equally criminal even without the use of a computer or electronic communication. It would, therefore, be better as a matter of basic principle for the Kenyan authorities to address such conduct by way of general provisions of the criminal law, rather than on a piecemeal basis.

- Secondly, the drafting of section 18 includes several vague provisions including "causing substantial emotional distress or anxiety to another person" by taking or distributing "pictures or photographs of any person without his consent" or displaying or distributing information "that substantially increases the risk of harm or violence to any other person". These latter provisions do not seem to us to be aimed solely at harassment or intimidation but could also very easily encompass a trade union organising an illegal blockade of a factory (threatening an illegal act and causing distress to the factory owners), or a photographer taking a picture of a politician involved in corrupt dealings (causing distress to the corrupt politician). The lack of any defence of reasonableness or public interest means that the proposed offence could easily be used to punish individuals engaged in entirely legitimate activities.

Recommendation:

- Section 18 of the Bill should be struck out in its entirety. Legislation against stalking and harassment should be dealt with by way of the general criminal law, rather than in the context of cybercrime.

Procedures and investigations

Part V sets out investigatory powers and procedures, including powers of access, search and seizure preservation order, expedited preservation, disclosure of data, production of data, collection of traffic data, interception and forensic tools. ARTICLE 19 does not propose to conduct a detailed analysis of this part of the Bill, which contains generally satisfactory safeguards for the protection of the rights to privacy and freedom of expression.

General provisions

Jurisdiction

Section 35 of the Draft Bill deals with the scope of application of the Bill. Section 35 (a) to (e) contains many common aspects of such jurisdictional clauses. We are very concerned, however, by Section 35 (f), which provides that the Kenyan courts have jurisdiction over any act or omission constituting an offence under the Bill is committed 'outside the territory or Kenya and where any result of the offence has an effect in Kenya'.

In our view, this is an unacceptably broad provision. It is unclear what 'effect' the offence should have in Kenya. For instance, Kenyan Internet users could be shocked by nude images available online that would be deemed obscene, vulgar, lewd or laviscious under Kenyan law. Because the images would have an 'effect' in Kenya, the person posting those pictures would be subject to the jurisdiction of the Kenyan courts despite the fact that he or she might be based in the United States and that this may not constitute an offence under US law.

Recommendations:

- Section 35 (f) should be removed.

General penalty

Section 40 provides for a general penalty of a fine not exceeding two million shillings or three-year imprisonment for committing any of the crimes laid down in the Bill.

This is a clear breach of the well-established criminal law principle of *non bis in idem*, i.e. that no one should be punished twice for the same crime. Accordingly, we strongly recommend that this provision should be struck out.

Recommendations:

- Section 40 should be removed

About ARTICLE 19

The ARTICLE 19 advocates for the development of progressive standards on freedom of expression and access to information at the international level, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available at http://www.article19.org/resources.php/legal/.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org. For more information about this analysis, please contact Gabrielle Guillemin, Legal Officer of ARTICLE 19 at gabrielle@article19.org or +44 20 7324 2500.

For more information about the work of ARTICLE 19 in Kenya, please contact Henry Maina, Director of ARTICLE 19 Kenya at henry@article19.org.

This analysis is wholly financed by the Swedish International Development Cooperation, Sida. Sida does not necessarily share the opinions here within expressed. ARTICLE 19 bears the sole responsibility for the content of the analysis.

Annex: Draft Cybercrime and Computer-Related Crimes Bill 2014

THE CYBERCRIME AND COMPUTER RELATED CRIMES BILL, 2014

ARRANGEMENT OF CLAUSES

Clauses

PART-IV-CONTENT RELATED OFFENCES

PART V – PROCEDURES AND INVESTIGATIONS

PART VI –GENERAL PROVISIONS

AN ACT of Parliament to prohibit unauthorized access, use or interference with a computer; to protect the integrity of computer systems and the confidentiality, integrity and availability of data; to prevent abuse of computer systems; to facilitate the gathering and use of electronic evidence; and connected purposes

ENACTED by the Parliament of Kenya—

PART I—PRELIMINARY

Short title.

1. This Act may be cited as the Cybercrime and Computer related Crimes Bill, 2014.

Interpretation.

2. In this Act, unless the context otherwise requires—

"access" in relation to any computer system", means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system;

"computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, software and communication facilities which are connected or related as a system or network;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device or collection of devices including input and output devices but excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions and data that perform logic, arithmetic, data storage, data retrieval, communication control and other functions;

"damage" means any impairment to a computer or the integrity or availability of data, program, system or information that—

(a) causes any loss;

(b) modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;

(c) causes or threatens physical injury or death to any person; or

(d) threatens public health or public safety;

"data" means information recorded in a format in which it can be processed by equipment operating automatically in response to instructions given for that purpose, and includes representations of facts, information and concepts held in any removable storage medium;

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities;

"electronic device", "acoustic device", or "other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

"electronic form" with reference to information, means any information generated, sent, received or stored in magnetic, optical, computer memory, microfilm or similar device;

"electronic record" means a record generated in digital form by an information system, which can be transmitted within an information system or from one information system to another and stored in an information system or other medium;

"equipment" includes any appliance, apparatus or accessory used or intended to be used for communication services;

"function" includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer;

"intercept in relation to a function of a computer", includes listening to, or recording a function of a computer, or acquiring the substance, its meaning or purport of such function;

"information" includes data, text, images, sounds, codes, computer programs, software and databases;

"information and communication technologies" means technologies employed in collecting, storing, using or sending out information and include those involving the use of computers or any telecommunication system;

"modification" means a modification of the contents of any computer system by the operation of any function of that computer system or any other computer system as a result of which—

(*a*) any program or data held in the computer system is altered or

erased;

(*b*) any program or data is added to its contents; or

(*c*) any act occurs which impairs the normal operation of the computer system;

"offence" in this Act, means an offence against a provision of any law in Kenya, or an offence against a provision of any law in a foreign state for conduct which, if it occurred in Kenya, would constitute an offence against a provision of any law in Kenya;

"person" includes any company or association or body of persons corporate or unincorporate;

"program" or **"computer program**" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function;

"traffic data" means any computer data relating to communication by means of a computer system generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.

PART II—OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS

Unauthorized access to computer data

3. (1) Subject to subsections (2) and (3), a person who causes a computer system to perform a function, knowing that the access they intend to secure is unauthorised, commits an offence and shall on conviction be liable to a fine not exceeding five hundred thousand shillings or to three years imprisonment or both

(2) Access by a person to any program or data held in a computer is authorised if—

(a) that person has the right to control the operation or use of the computer system and exercises such right in good faith;

(b) that person has the express or implied consent of the person, empowered to authorise them, to have such an access;

(c) that person has reasonable grounds to believe that they had such consent as specified in paragraph (b);

(d) that person is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of, any document or other property.

(3) An access by a person to a computer system is unauthorised if–

(a) that person is not himself entitled to control access of the kind in question; and

(b) does not have consent to access by him of the kind in question from any person who is so entitled.

(4) For the purposes of this section, it is immaterial that the unauthorised access is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

Access with intent to commit offences.

4. (1) A person who causes a computer system to perform any function for the purpose of securing access to any program or data held in any computer system, with intent to commit an offence under any law, that person commits an offence and is liable upon conviction to a fine not exceeding five hundred thousand shillings or to imprisonment term of two years or both.
(2) For the purposes of this section, it is immaterial that—

(*a*) the access referred to in subsection (1) is authorized or unauthorized;

(*b*) the further offence to which this section applies is committed at the same time when the access is secured or at any other time.

Unauthorized modification of computer data.

5. (1) A person who intentionally and without right—

(a) does any act which causes an unauthorised modification of the computer data; and

(2)Where as a result of the commission of an offence under subsection (1), the operation of the computer system, is impaired, or data contained in the computer system is suppressed or modified, the person convicted of such offence is liable on conviction to a fine not exceeding two hundred thousand shillings or to imprisonment for a term of two years or both.

(3) For purposes of this section modification is unauthorised if—

(a) the person whose act causes it, is not entitled to determine whether the modification should be made; and

(b) he or she does not have consent to the modification from a person who is entitled.

(4) For the purposes of this section, it is immaterial whether an unauthorized modification or any intended effect of it, be permanent or temporary.

Unauthorized access to and interception of computer service.

6. (1) Subject to subsection (2), a person who by any means knowingly:—

(*a*) secures access to any computer system for the purpose of obtaining, directly or indirectly, any computer service;

(*b*) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within a computer system, commits an offence is liable upon conviction to a fine not exceeding five hundred thousand shillings or to an imprisonment term of three years or both.

(2)Where as a result of the commission of an offence under subsection (1), the operation of the computer system, is impaired, or data contained in the computer system is suppressed or modified, the person convicted of such offence is liable on conviction to a fine not exceeding two hundred thousand shillings or to imprisonment for a term of two years or both.

(3) For the purpose of this section, it is immaterial that the unauthorized access or interception is not directed at—

(*a*) any particular program or data;

(*b*) a program or data of any kind; or

(*c*) a program or data held in any particular computer system.

(4) A person is not be liable under subsection (1) if—

(*a*) that person has the express or implied consent of both the person who sent the data and the intended recipient of such data;

(*b*) is acting in reliance of any statutory power.

Damaging or

7. (1) A person who without lawful authority or lawful excuse,

denying access to computer system.

does an act which causes directly or indirectly –

(a) a degradation, failure, interruption or obstruction of the operation of a computer system; or

(b) a denial of access to, or impairment of any program or data stored in, the computer system, commits an offence and shall be liable upon conviction to a fine not exceeding five million shillings or to an imprisonment term of three years or to both.

(2) For the purposes of this section, it is immaterial whether an unauthorized modification or any intended effect of it, is permanent or temporary.

Unauthorized disclosure of access code.

8. (1) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in any computer knowing or having reason to believe that it is likely to cause loss, damage or injury to any person or property, commits an offence.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding two hundred and fifty thousand shillings or to an imprisonment term of three years or to both.

System interference.

9. A person who, knowingly and without authority or lawful excuse—

(a) interferes with or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer,

commits an offence and is liable on conviction to a fine not exceeding two hundred and fifty thousand shillings or to an imprisonment term of three years or to both.

Illegal devices or data.

10. A person who knowingly manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a computer system or any other device or an designed or adapted primarily for the purpose of committing any offence under sections 1 to 9, shall commit an offence.

(2) A person who knowingly receives, or is in possession, without sufficient excuse or justification, of one or more of the devices under subsection (1) commits an offence.

(3) A person who is found in possession of any data or program with the intention that the data or program be used, by the person himself or another person, to commit or facilitate the commission of an offence under this Act, also commits an offence.

(4) For the purposes of subsection (3), possession of any data or program includes—

(*a*) having possession of a computer system or data storage device that holds or contains the data or program;

(*b*) having possession of a document in which the data or program is recorded; or

(*c*) having control of data or program that is in the possession of another person.

(5) A person who commits an offence under this section is liable upon conviction to a fine not exceeding one million shillings or to an imprisonment term of three years or to both.

Unauthorized receiving or giving access to a computer program or data.

11. (1) A person who receives or is given access to any program or data held in a computer and who is not authorised to receive or have access to that program or data whether or not the person knows that the person giving him the program or data has obtained that program or data through authorised or unauthorised means, commits an offence and is liable on conviction to a fine not exceeding five hundred thousand shillings or to imprisonment term of two years, or to both.

(2) A person who is authorised to receive or have access to any program or data held in a computer and who receives that program or data from another person knowing that the other person has obtained that program or data through unauthorised means commits an offence and is liable on conviction to a fine not exceeding one million shillings or to imprisonment term of three years, or to both.

(3) A person who has obtained any program or data held in a computer through authorised means and gives that program or data to another person who the person knows is not authorised to receive or have access to that program or data commits an offence and is liable on conviction to a fine not exceeding five hundred thousand shillings or to an imprisonment term not exceeding three years, or to both.

(4) A person who has obtained any program or data held in a computer through unauthorised means and gives that program or data to another person whether or not the person mows that that

other person is authorised to receive or have access to that program or data commits an offence and is liable on conviction to a fine not exceeding five hundred thousand shillings or to imprisonment for a term not exceeding two years, or to both.

PART III—COMPUTER RELATED OFFENCES

Computer related forgery.

12. (1) A person who intentionally and without lawful excuse or justification, inputs, alters, delays transmission, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, commits an offence and is liable upon conviction to a fine not exceeding ten million or ten years imprisonment or both.

(2) For purposes of subsection (1), it is immaterial whether or not the data is directly readable and intelligible.

Computer related fraud.

13. A person who intentionally and without lawful excuse or justification, causes the loss of property to another by—

(a) any input, alteration, deletion, delaying transmission or suppression of computer data;

(b) any interference with the functioning of a computer system,with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person, commits an offence and is liable upon conviction to a fine not exceeding five million or ten years or both.

Unauthorized access to protected system

14. A person who secures access or attempts to secure access to a protected system or computer in contravention of the provisions of this Part commits an offence and is liable upon conviction to a fine not exceeding one million shillings or an imprisonment term of five years, or both.

PART IV—CONTENT RELATED OFFENCES

Child pornography.

15. (1) Subject to section 16 (2) of the Sexual Offences Act, 2006, a person who—

Cap no. 3 of

(a) sells, lets to hire, distributes, publicly exhibits through a computer system and puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or their possession any obscene book, pamphlet, paper, drawing, painting, art, representation or figure or any other

obscene object;

(b) imports, exports or conveys any obscene object for any of the purposes specified in subsection (1), or knowingly or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited through a computer system and put into circulation;

(c) takes part in or receives profits from any business in the course of which they know or has reason to believe that any such obscene objects are, for any of the purposes specifically in this section, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited through a computer system and put into circulation;

(d) advertises or makes known through a computer system that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be produced from or through any person;

(e) offers or attempts to do any act which is an offence under this section, commits an offence of child pornography and is liable upon conviction is liable to imprisonment for a term of not less than six years or to a fine of not less than five hundred thousand shillings or to both and upon subsequent conviction, for imprisonment to a term of not less than seven years without the option of a fine.

(2)For the purposes of subsection (1), a book, pamphlet, paper, drawing, painting, art, representation or figure or any other object shall be considered to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or where it comprises two or more distinct items the effect of any one of its items, if taken as a whole, tends to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

(3) For purposes of this section, child pornography also includes pornographic material that visually depicts—

(a) a minor engaging in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct; or

(c) realistic images representing a minor engaged in sexually explicit conduct.

Hate speech.

16. (1) A person who—

(a) uses threatening, abusive or insulting words or behaviour,

(b) displays any written or electronic material;

(c) publishes or distributes written or electronic material; or

(d) distributes, shows or plays, a recording of visual images;

through a computer system which is threatening, abusive or insulting or involves the use of threatening, abusive or insulting words or behaviour whether publicly or anonymously, commits an offence if that person intends to stir up ethnic hatred, or having regard to all the circumstances, ethnic hatred is likely to be stirred up.

(2)It is immaterial where the offence referred to in subsection (1) is conducted privately or publicly.

(3) A person who commits an offence under this section shall be liable upon conviction to a fine not exceeding one million shillings or to an imprisonment term for a term not exceeding five years or to both. In this section, "ethnic hatred" means hatred against a group of persons defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins.

Identity related crimes.

17. (1) A person who, intentionally and without lawful excuse or justification by using a computer system at any stage of the offence, transfers, possesses, or uses any means of identification of another person, with the intent to commit, aid or abet, in connection with, any unlawful activity that constitutes a crime, commits an offence.

(2) A person is liable upon conviction under subsection (1) to a fine not exceeding five hundred thousand shillings or to an imprisonment term of five years or both.

Cyberstalking

18. (1) A person who willfully, maliciously, and repeatedly uses a computer system including electronic communication to harass, intimidate or cause substantial emotional distress or anxiety to another person—

(a) makes a threat with the intent to place that person in reasonable fear for their safety or to a member of that person's immediate family;

(b) communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, picture or image;

(c) make any suggestion or proposal of an obscene nature;

(d) threaten any illegal or immoral act;

(e) take or distribute pictures or photographs of any person without his consent or knowledge;

(f) display or distribute information in a manner that substantially increases the risk of harm or violence to any other person,

commits the offence of cyber stalking.

(2) A person who is convicted of the offence referred to in section (1) is liable to a fine not exceeding three hundred thousand shillings or to an imprisonment term of three years or both.

(3) If the offence referred to in subsection (1) involves a minor, the penalty is a fine not exceeding five hundred thousand shilling s or to an imprisonment term of ten years or both.

Phishing.

19. (1) A person who establishes a website, or sends an electronic message with a counterfeit source intended to deceive the recipient or visitor or its electronic system to be an authentic source with intent to gain unauthorized access or obtain valuable information which later may be used for unlawful purposes commits the offence of` phishing.

(2) A person who commits an offence of phishing upon conviction is liable to a fine not exceeding five hundred thousand shillings or to an imprisonment term of three years or both.

(3) Where the phishing attack results in economic gain for the sender, the penalty upon conviction is a fine not exceeding five million shillings or an imprisonment term of seven years or both.

Spamming

20. (1) A person who, intentionally without lawful excuse or justification—

(a) intentionally initiates the transmission of multiple electronic mail messages from or through such computer system;

(b) uses a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or Internet service provider, as to the origin of such messages, or

(c) materially falsifies header information in multiple electronic mail messages and intentionally initiates the transmission of such messages,

commits an offence is liable upon conviction to an imprisonment term for a period not exceeding three years, or to a fine not exceeding five hundred thousand shillings or to both.

(2) This section shall not apply to the transmission of multiple electronic messages within customer or business relationships.

Offences by body corporate.

21. (1) Where a body corporate is held liable for an offence under this Act if the offence is committed on its instructions or for its benefits. The body corporate shall be punished with fine not exceeding fifty million shillings or the amount involved in the offence whichever is the higher.

(2) Where a corporation is convicted of an offence, or is fined under this Act, any person who is a director of, or who is concerned in the management of that corporation shall be considered to have committed the same offence and is liable to be fined as if the person authorized or permitted the same or omission constituting the offence—

(3) Where at the trial of a corporation for an offence under this Act, a director or any person concerned in the management of that body corporate shows that—

(a) the act constituting the offence was done without the knowledge or consent of that director or person; or

(b) the director or person took, reasonable steps to prevent the act from being committed;

the director or person shall not be liable.

Abatements and attempts.

22. (1) A person who abets another person in committing an offence under this Act, commits that offence and is liable on conviction to the punishment prescribed for the offence.

(2) A person who attempts to commit any offence under this Act commits that offence and is liable on conviction to the punishment prescribed for the offence.

Attempts.

23. (1) When a person, intending to commit an offence, begins to put their intention into execution by means adapted to its fulfilment, and manifests their intention by some overt act, but do not fulfil their intention to such an extent as to commit the offence, they are considered to attempt to commit the offence.

(2) It is immaterial, whether the person does all that is necessary on their part for—

(a) completing the commission of the offence;

(b) whether the complete fulfillment of their intention is prevented by circumstances independent of their will; or

(c) whether they desists of their own motion from the further prosecution of

their intention.

(3) It is immaterial that by reason of circumstances not known to the offender it is impossible in fact to commit the offence

PART V—PROCEDURES AND INVESTIGATIONS

Powers of access, search and seizure

24. (1) Where a court is satisfied on the basis of an application by a Police officer or lawful authority supported by information on oath that there are reasonable grounds to believe that there may be in a place a thing or computer data—

(a) that may be material as evidence in proving an offence; or

(b) that has been acquired by a person as a result of an offence.

(2)On the basis of an application made under subsection (1), the court may issue a warrant authorizing a police Officer or lawful authority, to enter any premises to access, search and seize the thing or computer data including—

(i) a computer system or part of it and computer data stored therein; and

(ii) a computer-data storage medium in which computer data may be stored in the territory of the country.

(3) Where a police officer or lawful authority acting under a warrant issued under subsection (2) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the police officer or lawful authority must expeditiously extend the search or access to the other system.

(4) A Police Officer or lawful authority undertaking a search under this section is empowered to seize or secure data accessed.

Preservation order.

25. (1) A police officer or lawful authority may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

(2) For the purpose of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) shall remain in force—

(a) until such time as may reasonably be required for the investigation of an offence; or

(b) where prosecution is instituted, until the final determination of the case or until such time as the court considers appropriate.

Expedited preservation.

26. (1) If a police officer or lawful authority is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the police officer may, by written notice given to a person in control of the data, require the person to ensure that the data specified in the notice be preserved for a period of up to ninety (90) days as specified in the notice.

(2) The period may be extended beyond ninety days upon an application a court authorizes an extension for a further specified period of time.

(3) A preservation notice comes into force when the carrier receives the directive or order as the case may be.

Disclosure of data.

27. A police officer or lawful authority may, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of—

(a) all preserved or specified data stored or processed by means of a computer system or any other information and communication technologies, irrespective of whether one or more service providers were involved in the transmission of such data; or

(b) sufficient data to identify the service providers and the path through which the data was transmitted.

Production order.

28. (1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, a police officer or lawful authority may apply to court for an order compelling—

(a) a person to submit specified data in that person's possession or control, which is stored in a computer system; and

(b) a service provider offering its services to submit subscriber

information in relation to such services in that service provider's possession or control.

(2) Where any material to which an investigation relates consists of data stored in a computer, computer system or preserved by any mechanical or electronic device, the request shall be considered to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

Collection of traffic data.

29. (1)If a court is satisfied on the basis of an application by a police officer or lawful authority, supported by information on oath, that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the court may order a person in control of such data to—

(a) collect or record traffic data associated with a specified communication during a specified period; or

(b) permit and assist a specified law enforcement officers to collect or record that data.

(2)If a court is satisfied on the basis of an application by a police officer or lawful, supported by information on oath that there are reasonable grounds to suspect or believe that traffic data is reasonably required for the purposes of a criminal investigation, the court may authorize the police or prosecutions officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Interception of traffic data.

30. If a court is satisfied on the basis of an application by a police officer or lawful authority, supported by information on oath, that there are reasonable grounds that traffic data is reasonably required for the purposes of a criminal investigation, the court may authorize a police officer or lawful authority to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Obligation to report data loss.

31. (1) All public or private corporations processing personal data shall as soon as practicable report any security breaches resulting in theft, loss or misuse of data to the police.

(2) A public or private corporation who fails to comply with subsection (1) commits an offence.

Interception of content data.

32. If a court is satisfied on the basis of an application by a police officer or lawful authority supported by information on oath that there are reasonable grounds to believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the court may—

(a) order a service provider whose service is available in Kenya through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

(b) authorize a police officer or lawful authority to collect or record that data through application of technical means.

Forensic tools.

33. (1) If a court is satisfied on the basis of an application by a police officer or lawful authority, supported by information on oath that in a criminal investigation concerning an offence under this Act, there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments and is reasonably required for the purposes of a criminal investigation, the court may authorize the police officer or lawful authority to utilize a remote forensic tool with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information—

(a) suspect of the offence, if possible with name and address;

(b) description of the targeted computer system;

(c) description of the intended measure, extent and duration of the utilization, and

(d) reasons for the necessity of the utilization.

(2) Within such investigation, the police officer or lawful authority must ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation process it is necessary

to—

(a) the technical mean used and time and date of the application;

(b) the identification of the computer system and details of the modifications undertaken within the investigation;

(c) any information obtained.

(3) Information obtained by the use of such tool need to be protected against any modification, unauthorized deletion and unauthorized access.

(4) The duration of authorization in this subsection (1) is limited to nine months. If the conditions of the authorization are no longer met, the actions taken are to stop immediately.

(5) The authorization to install the tool includes remotely accessing the suspect's computer system.

(6) If the installation process requires physical access to a place the requirements of section 23 need to be fulfilled.

(7) If necessary a police officer may pursuant to the order of court granted in subsection (1) request a service provider to support the installation process.

Duty to cooperate.

34. (1) A person who is required to cooperate with police or lawful authority in their discharge of functions under this Act or any other written law, and shall in particular—

(a) respond to any inquiry;

(b) comply with any lawful directions including disclosing access code to a computer system or computer; and

(c) furnish such information as may be required;

(2) A person who contravenes subsection (1) is be liable upon conviction, to an imprisonment term of one year or to a fine not exceeding three hundred thousand shillings or to both.

(3) In addition to the penalty prescribed under subsection (2), a public officer or State officer may be subjected to the relevant disciplinary procedures.

PART VI—GENERAL PROVISIONS

Jurisdiction

35. The Kenyan courts shall have jurisdiction where an act done or an omission made constituting an offence under this Act has been committed—

(a) in the territory of Kenya;

(b) by a national of Kenya outside the territory of Kenya

(c) on a ship or aircraft registered in Kenya;

(d) in part in Kenya;

(e) using a Kenyan domain name; or

(f) outside the territory of Kenya and where any result of the offence has an effect in Kenya.

Admissibility of electronic evidence.

36. The fact that evidence has been generated from a computer system does not by itself prevent that evidence from being admissible.

Confiscation of assets.

37. A court may order the confiscation of moneys, proceeds, properties and assets purchased or obtained by a person with proceeds derived from or in the commission of an offence under this Act and may further make an order of restitution.

International cooperation.

38. The Provisions of the Mutual Legal Assistance Act, 2011shall apply to this Act.

Protection from personal liability.

39. No act done by a person exercising a function in this Act shall, if the act was done in good faith for the purpose of carrying out the provision of this Act, subject the person to any liability, action, claim or demand.

General penalty.

40. A person who contravenes any provisions of this Act commits an offence and shall be liable upon conviction to a fine of not exceeding two million shillings or to imprisonment term of three years or both.

Regulations.

41. The Cabinet Secretary for the time being responsible for matters relating to information, communication and technology may, in consultation with the Director of Public Prosecutions make regulations regarding any matter provided under this Act.