ARTICLE 19

Tanzania: Cybercrime Act 2015

May 2015

Legal analysis

Executive summary

In May 2015, ARTICLE 19 analysed the Tanzanian Cybercrimes Act 2015 (the Act). The Act, adopted on 1 April 2015, has drawn much criticism from political opposition inside the country as well as from national and international human rights groups. As a result, the government of Tanzania has committed to revising the Act before the end of this Parliamentary session.

ARTICLE 19 welcomes the announcement of this review process. This analysis has been prepared with a view to assisting the government with its revision of the Act to ensure that it fully complies with international standards on freedom of expression.

Our analysis has identified a number of areas of serious concern from an international law perspective. Our concerns lie not only in relation to content and computer-related offences but also in relation to the lack of adequate procedural safeguards, the Act's disproportionate and inflexible sanctions regime, and the conveyance of excessive powers to police forces to conduct search and seizure operations without judicial oversight, amongst others.

Key recommendations:

- The Act should include sufficient safeguards for protection of human rights, including the due process of law.
- Given the format of the Act, all specific references to sanctions should be removed. Instead, a new section, on 'Sanctions and Measures,' should be drafted that clearly categorises offences and lists effective, proportionate and dissuasive sanctions that, where appropriate, take into account intention, dishonesty, the seriousness of an offence and any available defence; including, public interest defences. All references to minimum sanctions should be removed and maximum penalties should be introduced instead;
- Clear and precise provisions should be included within Sections 4-7 of the Act that require dishonest intent in their commission and serious harm to result before criminal liability attaches;
- Public interest defences should be made available to ensure that legitimate whistleblowers acting in good faith are not prosecuted under the Act;
- The definitions of key terms should be revised while vague and overbroad terms, such as 'lascivious' and 'obscene' in Section 14, should be removed;
- Section 4 should be amended to include 'dishonest' intent to 'obtain computer data;'
- Section 5 should be struck out in its entirety;
- Section 6 should be amended to clarify that any intention to illegally intercept data should be dishonest;
- Sections 7(1) and (2) should be amended to include reference to the need for serious harm to have resulted from the commission of an offence before criminal liability attaches;
- Section 7(1)(f) should be struck out;
- Section 7(1)(g) should be amended to make specific reference to denial of access via electronic means, or physical interference with computer systems or networks;
- Provisions requiring that the commission of an offence under Sections 7(2)(a) and (b) be done intentionally and unlawfully should be included and a public interest defence must be made available to protect whistleblowers;
- Section 8 should be redrafted to clarify in more precise terms that any 'unauthorised' access must be unlawful, intentional and result in serious harm in order for criminal liability to arise;
- Section 9 should be redrafted to make explicit reference to the need for intentionality and the 'serious hindering without right' of the functioning or usage of a computer system;
- Section 10 should be redrafted; at the very least, a requirement of intentionality should be included and the list of offences to which the provision applies should be explicitly set out.

The title of the Section should be changed from 'illegal device' to 'misuse of devices' to reflect the fact that the mere possession of an electronic device is not an offence but rather the intention with which it is used;

- Section 11 should be amended to include a requirement for dishonest intent before criminal liability attaches;
- The phrase, 'with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person' should be included after Section 12(1)(b);
- Section 13 should be amended to clarify that offences must be unlawfully committed with intent;
- Sections 14, 15, 16 and 20 should be struck out in their entirety;
- Sections 17-19 should be removed from the Act and the offences they establish should be clearly set out at more appropriate parts of the criminal law;
- Section 23 should be struck out. Legislation against harassment, coercion and intimidation should be dealt with under broader criminal law, containing clearly defined terms to ensure that the provisions are lawful and that clearly defined public interest and reasonableness defences are available to protect legitimate forms of freedom of expression;
- Non-commercial infringements of intellectual property rights should be abolished;
- In relation to commercial offences, Section 24 should be revised;
- Sections 25-27 should be merged and rephrased; a *mens rea* requirement of intentionality should be included for the offences set out in Sections 25 and 27;
- Section 29 should be struck out and instead be listed as an aggravating factor under a sanctions Section/Part;
- To clarify the limitations of police powers under Part IV of the Act, all references to the word 'may' in relation to the discretion of police officers to apply to the court for an order permitting them to execute their powers under Part IV should be replaced with the word 'must' to secure adequate judicial oversight. Specifically, the word 'may' should be replaced with the word 'must' within Sections 32(3), 33(2), 36 and 37(1);
- Within Section 36, the specification that a police officer 'may' apply to the court for an order only in instances where his powers cannot be executed without the threat of the use of force should be removed entirely and replaced with a specific requirement that a police officer in charge of a police station must apply to the court for order for the execution of any of his powers under Section 36 and Part IV more broadly;
- Part IV should be amended to specify that powers within Part IV should only be applied in relation to specified serious offences;
- Section 39(2) should be amended to clarify that any procedures that are developed should be proactively published;
- The burden of proof set out at Section 39(3) should be reversed and it should be for the prosecution to prove beyond reasonable doubt, on a case-by-case basis, that an intermediary illegally disclosed data;
- Sections 39(4) and 40 should be struck out;
- All references to 'competent/relevant authorities' should be removed (from Sections 41(1)(a), 42(e) and 43(a)). The terms should be replaced with a provision that makes clear that information shall only be removed by providers upon receipt of a court order, which has been made following an application made to the court setting out grounds showing reasonable suspicion or probable cause that a serious specified offence has been committed. Furthermore, where appropriate, as decided by a court of law, a suspect shall have the right to hear the application against him and file a defence.
- The notice and take down regime should be abolished. As an alternative, a notice-to-notice regime could be established;
- Section 49 should be amended, specifically to include that no person shall be held liable unless there is clear evidence of illegal conduct against them; and
- The evidential burden of proving illegal conduct should be reversed to lie with the prosecution to prove beyond reasonable doubt that an offence was committed.

Table of contents

Introduction

On 1 April 2015, Tanzania's Parliament passed the Cybercrimes Act 2015 (the Act).[1] Since its enactment, the Act has drawn much criticism from political opposition inside the country as well as from national and international human rights groups.[2] As a result, the Government of Tanzania has committed to revising the Act before the end of this Parliamentary session.

ARTICLE 19 welcomes the announcement of this review process and hopes that this analysis will assist the Tanzanian Government its revision. ARTICLE 19 is well place to undertake this analysis thanks to our extensive experience of working on freedom of expression issues in Africa, including working on issues related to the protection of freedom of expression online. We have analysed several cybercrime laws from around the world including in Kenya[3], Brazil[4], Iran[5], Pakistan[6] and Cambodia[7] and as a result are particularly well placed to analyse the Act.

ARTICLE 19's analysis first sets out in detail the international standards in relation to freedom of expression, the right to privacy, and cybercrime, together with guidance on how these provisions are interpreted in relation to information and communication technologies. It then goes on to make a number of general recommendations regarding the Act as a whole before highlighting human rights issues with particular sections of the Act.

The analysis not only highlights concerns and conflicts with international human rights standards within the Act but also actively seeks to offer constructive recommendations on how the Act can be improved. We explain the ways in which problematic provisions in the Act can be made compatible with international standards on freedom of expression and privacy and set out key recommendations at the end of each section.

[1] The analysis was undertaken in reference to the English language version of the Act only and our comments and recommendations relate only to that version. The text of the Act is available at http://bit.ly/1HOPOB7.
[2] See for example: Global Voices, *Tanzania's Cyber Crime Bill Gives More Power to Police, Less to People*, 17 April 2015, available at http://bit.ly/1CUvtVq; Pesa Times, *Activists Criticize Cybercrimes Law*, 5 April 2015, available at http://bit.ly/1JP6d85; or CIPESA, *Tanzania Cybercrime Bill Should Safeguard Citizens' Rights on the Internet*, 2 April 2015, available at http://bit.ly/1Recdyd.
[3] ARTICLE 19, Kenya: Cybercrime and Computer Related Crimes Bill, July 2014, available at http://bit.ly/1HOPICH.
[4] ARTICLE 19, Brazil: Draft Cybercrimes Law, January 2012, available at http://bit.ly/1Recz81.
[5] ARTICLE 19, Islamic Republic of Iran: Computer Crimes Law, 2012, available at http://bit.ly/1RecP6R.
[6] ARTICLE 19 and Digital Rights Foundation Pakistan, Pakistan: New Cybercrime Bill Threatens the Rights to Privacy and Free Expression, 2014, available at http://bit.ly/1G1LSrh.
[7] ARTICLE 19, Cambodia: Secret Draft Cybercrime Law seeks to undermine free speech online, April 2014, available at http://bit.ly/1HFOfp7.

International human rights standards

The right to freedom of expression in international law

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

Moreover, freedom of expression is guaranteed in the **African Charter on Human and Peoples' Rights** (ACHPR)[10] and in the **Declaration of Principles on Freedom of Expression in Africa** (African Declaration).[11]

Additionally, **General Comment No 34**,[12] adopted by the UN Human Rights Committee (HR Committee) in 2011, explicitly recognises that Article 19 ICCPR protects all forms of expression and the means of their dissemination, including 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 (e.g. Internet and mobile-based electronic information dissemination systems) have dramatically changed communication practices.[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]

Further useful interpretative commentary on the application of Article 19 of the ICCPR is found in the 2011 **Joint Declaration on Freedom of Expression and the Internet**[16] (the 2011 Joint Declaration) of the four freedom of expression special mandates, including the African Special Rapporteur on Freedom of Expression and Access to Information. It reaffirms that freedom of expression applies to the internet and, *inter alia*, recommends 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, and promoting the use of self-regulation as an effective tool in redressing harmful speech.

As a State party to the ICCPR and the African Charter, Tanzania is required to adhere to the above provisions and guidance when formulating domestic legislation, including legislation that regulates electronic and Internet-based modes of expression.

Permissible restrictions on the right to freedom of expression

The right to freedom of expression is a fundamental right but it is not guaranteed in absolute terms: any restriction on the right should meet so-called "three part test," developed by the HR Committee. Namely, restrictions must:

[8] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[9] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[10] Organization of African Unity (OAU), *African Charter on Human and Peoples' Rights ("Banjul Charter")*, 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), Article 9.
[11] Adopted at the 32nd Session of the African Commission on Human and Peoples' Rights, 17-23 October 2002, Article 11.
[12] CCPR/C/GC/3, adopted on 12 September 2011, available at http://bit.ly/1xmySgV.
[13] *Ibid*, para. 12.
[14] *Ibid*, para. 17.
[15] *Ibid*, para. 39.
[16] Joint Declaration on Freedom of Expression and the Internet, June 2011, available at http://bit.ly/1CUwVap.

- **Be 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 in 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;

- **Be necessary and proportionate** to secure the legitimate aim: 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 tailored to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.[18] Furthermore, it should be noted that the imprisonment of individuals, "for seeking, receiving or imparting information and ideas can rarely be justified as a proportionate measure to achieve one of the legitimate aims under article 19, paragraph 3 [...]."[19]

Further limitations on the right to freedom of expression are stipulated in Article 20 para 2 of the ICCPR which requires states to prohibit "any *advocacy* of national, racial or religious hatred that constitutes *incitement* to discrimination, hostility or violence shall be prohibited by law." Article 20 para 2 of the ICCPR does not require States to prohibit all negative statements towards national groups, races and religions. However, States should be obliged to prohibit the advocacy of hatred that constitutes incitement to discrimination, hostility or violence. "Prohibition" allows three types of sanction: civil, administrative or, as a last resort, criminal.

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[20] This clarification is reaffirmed in both the African Declaration[21] and the Joint Declaration.[22]

Online content regulation

The above principles have been endorsed and further explained in the two reports[23] prepared by the UN Special Rapporteur on the right to freedom of opinion and expression (Special Rapporteur on FOE). In his August 2011 report, the Special Rapporteur on FOE clarified the scope of legitimate restrictions on different types of expression online.[24] He 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

[17] HR Committee, *L.J.M.de Groot v. The Netherlands*, No. 578/1994, UN Doc.CCPR/C/54/D/578/1994 (1995).
[18] HR Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[19] Report of the UN Special Rapporteur on Freedom of Expression, A17/27, 17 May 2011 (May 2011 Report of Special Rapporteur), para 36,
[20] General Comment 34, op.cit., para 43.
[21] African Declaration, *op.cit.,* Article II. Also, Article XIII recommends that, "[s]tates shall review all criminal restrictions on content to ensure that they serve a legitimate interest in a democratic society."
[22] The 2011 Joint Declaration, para 1a.
[23] May 2011 Report of Special Rapporteur and Report of the UN Special Rapporteur on Freedom of Expression, A/66/290, 10 August 2011.
[24] *Ibid*, August report, para 18.

- expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[25]

In particular, the Special Rapporteur on FOE 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.[26] 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. The above restrictions must also conform to, and meet the requirements of, the three-part test.[27] No other category of expression may be lawfully restricted.[28]

Role of Internet intermediaries and intermediary liability

The special mandates have also commented on the role and measures available to intermediaries to censor online content. In relation to intermediaries, the Special Rapporteur on FOE noted that:

> Holding intermediaries liable for the content disseminated or created by their users severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads to self-protective and over-broad censorship, often without transparency and the due process of the law.[29]

Similarly, on notice-and-takedown systems, he commented that:

> [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 over-censoring 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.[30]

Accordingly, the four special mandates recommended in their 2011 Joint Declaration that:

- 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;
- Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online; and

[25] *Ibid.*
[26] May 2011 report, para 25.
[27] August 2011 report, *op.cit.,* para 3.
[28] August 2011 report, *op.cit.,* para 40.
[29] May 2011 report, *op.cit.,* para 40
[30] May 2011 report, *op.cit.,* para 42.

- Internet service providers (ISPs) and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown.[31]

The Special Rapporteur on FOE also recognised the need for strong procedural safeguards "against abuse, including the possibility of challenge and remedy against [any restriction's] abusive application."[32] He also stated that the arbitrary use of criminal law to sanction legitimate expression constitutes one of the gravest forms of restriction to the right [of freedom of expression], as it not only creates a "chilling effect", but also leads to other human rights violations, such as arbitrary detention and torture and other forms of cruel, inhuman or degrading treatment or punishment."[33]

Surveillance of communication

The right to privacy complements and reinforces the right to freedom of expression. The right to privacy is essential for ensuring that individuals are able to freely express themselves, including anonymously,[34] should they so choose. 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 to private communications is strongly protected in international law through Article 17 of the ICCPR,[35] that *inter alia*, states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family or correspondence. In **General Comment no. 16** on the right to privacy,[36] the HR Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives the ICCPR. It further stated that:

> [E]ven 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 authorised interference must be made only by that authority designated under the law, and on a case-by-case basis.[37]

The UN Special Rapporteur on the 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:

> Article 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.[38]

---

[31] 2011 Joint Declaration, *op.cit.,* para 2a and b.
[32] The May 2011 report, *op.cit.,* para 69.
[33] *Ibid.*, para 28.
[34] *Ibid.*, para 84.
[35] 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.
[36] General Comment 16, adopted 8 April 1988.
[37] *Ibid.*, para 8.
[38] 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, para 17.

In terms of surveillance (within the context of terrorism in this instance), he defined the parameters of the scope of legitimate restrictions on the right to privacy in the following terms:

> 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 the 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.[39]

The Special Rapporteur on FOE has also observed that:

> The right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of the administration of criminal justice, prevention of crime or combatting 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 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.

Cybercrime and international law

No international standard on cybercrime exists in the area. From the regional standards, the 2001 Council of Europe Convention on Cybercrime (the Cybercrime Convention), in force has entered in force in July 2004, has been the most relevant standard.[40] Although Tanzania is not a signatory to the Convention, it provides a helpful model for states seeking to develop cybercrime legislation.

The Convention provides definitions for relevant terms, including definitions for: computer data, computer systems, traffic data and service providers. It requires State parties to create offences against the confidentiality, integrity and availability of computer systems and computer data; computer-related offences including forgery and fraud; and content-related offences such as the criminalisation of child pornography. The Convention then sets out a number of procedural requirements for the investigation and prosecution of cybercrimes, including preservation orders, production orders and the search and seizure of computer data.

Importantly, the Convention makes it clear that the above measures must respect conditions and safeguards for the protection of human rights and liberties, consistent with the ICCPR and other applicable international human rights instruments.

[39] 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, paragraph 21

[40] The Council of Europe Convention on Cybercrime, CETS No. 185. As of May 2015, 46 states have ratified the Convention and a further eight states have signed the Convention but have not ratified it.

Analysis of the Cybercrimes Act 2015

The Act is made up of seven parts with a total of 59 sections. Part I covers preliminary provisions; Part II, provisions relating to offences and penalties; Part III, jurisdiction; Part IV, provisions relating to search and seizure; Part V, the liability of service providers; Part VI, general provisions, including offences committed by corporate bodies; and, Part VII, consequential amendments to other Acts of Parliament.

The following part of this analysis is divided into general comments and recommendations that relate to the Act as a whole, and specific comments and recommendations that identify problematic issues that are particular to specific provisions under the Act.

General comments

Before analysing the provisions of the Act in detail, ARTICLE 19 makes the following general observations about the Act:

- **Unclear structure of the Act:** Parts II (containing 25 provisions on various offences and penalties) and IV (entitled "search and seizure" but covering cover a number of procedural law elements) are particularly unclear. The manner in which these two Parts of the Act are set out is confusing and does not follow a logical sequence. For example, in Part II, provisions dealing with the disclosure of details of an investigation (Section 21) and the obstruction of an investigation (Section 22), appear between provisions on unsolicited messages (Section 20) and cyber bullying (Section 23). Similarly, in Part IV on search and seizure, provisions relating to the acquisition of a court order (Section 36) appear between provisions relating to the disclosure and collection of content data (Section 35) and the use of a forensic tool (Section 37). Section 38 then sets out provisions relating the hearing of an application.

- **Lack of procedural safeguards**: procedural safeguards for human rights protection are markedly absent throughout the Act. In particular, there is no reference at all to Tanzania's obligations to uphold and protect the right to freedom of expression and the right to privacy under the ICCPR and African Charter. ARTICLE 19 finds that the absence of any such provisions could threaten the entire Act's compatibility with international human rights standards and the enforcement of human rights in this area.[41]

- **Disproportionate sanctions**: In general, the Act imposes a disproportionate, inflexible and, at times, irrational sanctions regime. The sanctions, more often than not, lack any *mens rea* requirement of dishonest intent, or any requirement that serious harm should flow from the commission of an offence before criminal liability attaches; contrary to best practices in international law. ARTICLE 19 observes that minimum financial and custodial sanctions are imposed throughout the Act, which in effect prevent a court of law from exercising its discretion in the balancing of aggravating and mitigating factors during sentencing proceedings on a case-by-case basis. Moreover, a harm test or the availability of public interest defences is not provided within the Act where appropriate.[42]

[41] *C.f.,* May 2011 report, para 69, which recognised need for strong procedural safeguards "against abuse, including the possibility of challenge and remedy against [any restriction's] abusive application."
[42] *Ibid.*, para 36, which stated that the incarceration of individuals, "for seeking, receiving or imparting information and ideas can rarely be justified as a proportionate measure to achieve one of the legitimate aims under article 19, paragraph 3 [of the ICCPR] [emphasis added]."

Furthermore, throughout the Act there are numerous instances of inflexible sanctions being imposed for offences. For example, the minimum term of incarceration for 'attempt' is six months (Section 26(3)), whereas the minimum term for 'conspiracy' is one year (Section 27), despite the fact that greater (hypothetical) harm is likely to have resulted from the attempted commission of an offence than it is from a conspiracy to commit an offence. Additionally, a minimum term of incarceration of 'not less than three years' is prescribed for the non-commercial violation of another's intellectual property rights; notwithstanding that there is no requirement of intentionality, dishonesty or that any serious harm, or even financial loss, result.

- **Excessive police powers in Part IV of the Act**: ARTICLE 19 observes that Section 31 (provisions on the search and seizure of computer systems, devices or data) confers excessive discretionary power upon relatively low-ranking police officers without judicial oversight. There is no requirement that a police officer must obtain a court order to conduct search and seizure operations, which are a serious infringement on an individual's right to privacy. These excessive powers are compounded by the absence of sufficiently robust procedural safeguards throughout the Act, as mentioned above, or the availability of any means of challenging search and seizure procedures. These provisions run counter to international standards that stipulate that a law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution.[43]

- **Insufficient protection for whistleblowers**: Sections 4-7 of the Act, on illegal access, remaining, interception and interference, when read together, allow for the prosecution of potential whistleblowers, in violation of international standards. Section 7(2) is particularly troubling in this regard as it criminalises the communication, disclosure or transmission of any computer data, program, access code or command to an unauthorised person without any requirement that there be dishonest intent, or that serious harm should result. Furthermore, no public interest defences are available.

Recommendations:

- In order to clarify its provisions and also facilitate the criminal justice process in any international or cross-border case that may arise, Part II and Part IV of the Act should be reorganised into separate headings covering different topics;
- The Act should include sufficient safeguards for the protection of human rights, including due process provisions (preferably emulating Article 15 of the Cybercrime Convention). All the powers conferred on Tanzanian authorities under Part IV of the Act should then specifically refer to the new provision. All powers conferred upon the police should also be made subject to the acquisition of an order from a court following the submission of an application by the police setting out reasonable grounds or probable cause. Where appropriate, as decided by a competent court on a case-by-case basis, a suspect should be allowed to challenge the application.
- Given the format of the Act, all specific references to sanctions should be removed. Instead, a new Part on 'Sanctions and Measures,' should be drafted that clearly categorises offences and lists effective, proportionate and dissuasive sanctions that, where appropriate, take into account intention, dishonesty, the seriousness of an offence and any available defence; including, public interest defences. All references to minimum sanctions, both financial and periods of incarceration, should be removed from the Act and discretion as to the appropriate level of sanction left to a competent and impartial court. Maximum penalties - rather than minimum ones - should be introduced.

[43] General Comment 34, *op.cit.*, para 25.

- Clear and precise provisions should be included within Sections 4-7 of the Act that require dishonest intent in their commission and serious harm to result before criminal liability attaches.
- Public interest defences should be made available to ensure that legitimate whistleblowers acting in good faith are not prosecuted under the Act.

Specific comments

Section 3: Interpretation (definitions)

In general, ARTICLE 19 welcomes that this section sheds some light upon the meaning of key operative terms. In particular, it contains the definition of some key terms (e.g. 'computer data'), which uses very similar language to the definition within the Cybercrime Convention. Nonetheless, there are several definitions that we believe could be strengthened, as well as a number of definitions that could be added to facilitate clearer interpretation of the Act. In particular:

- The definition of 'computer system' omits the words 'automatic processing', which – for comparative reasons - is a key component of the Cybercrime Convention's definition;

- The definition for 'service provider' is insufficiently precise. Firstly, it mentions 'information system services' which itself is not defined in Section 3. Secondly, it fails to specify that service providers may be either public or private entities that provide users the ability to communicate by means of a computer system, or any other entity that processes or stores computer data on behalf of such communication users;

- Within the definition of 'Minister' we recommend that the words 'for the time being' be removed as they impliedly refer solely to the incumbent Minister as opposed to the Office of the Minister for Information and Communication;

- The term 'pornography' is not defined. Moreover, the terms 'lascivious' and 'obscene' (Section 14) are not defined either. Notwithstanding our specific comments on Section 14 (below), definitions for these terms should be included or reference be made to the relevant legislation in which definitions for the terms already exist;

- The definition of 'law enforcement officer' includes 'any other person authorised in any written law'. We find this definition too broad – it may inadvertently confer powers upon persons to whom it does not intend to; and

- Finally, it would be helpful if Section 3 were to include references to other legislation in which key operative terms are defined. For example, it would help clarify Act if reference were made to the relevant legislation in which the terms 'trademark', 'patent' and 'copyright' were defined in Tanzanian law.

Recommendations:

- The definitions of 'computer system' and 'service provider' should be aligned with those under the Cybercrime Convention;
- The definition of 'traffic data' (Section 34) should be moved to Section 3 for ease of reference;
- Vague and overbroad terms, such as 'lascivious' and 'obscene' in Section 14, should be removed;
- The definition of 'law enforcement officer' that disturbingly includes 'any other person authorised in any written law' should removed from the Act; and
- References to other legislation in which key operative terms are defined should be included in the Act.

Sections 4-6: Illegal access, remaining and interception

Section 4 criminalises the intentional and unlawful access of a computer system. The provision is overly broad and does not include reference to the need for security measures to have been infringed or 'dishonest' intent to 'obtain computer data' to have occurred.

Section 5 criminalises the intentional and unlawful 'remaining' within a computer system. It is unclear how this Section differs in substance to Section 4 above, as to illegally remain within a computer system, one must first illegally have accessed it.

Section 6 criminalises the intentional and unlawful interception by technical means of non-public transmissions of data. Again, ARTICLE 19 notes the absence of a requirement that any intent be dishonest.[44]

Recommendations:

- Section 4 should be amended to include 'dishonest' intent to 'obtain computer data;'
- Section 5 should be struck out in its entirety; and
- Section 6 should be amended to clarify that any intention to illegally intercept data should be dishonest.

Section 7: Illegal data interference

This section is divided into three subsections covering the (1) intentional and unlawful damage or deletion of computer data, (2) the transmission of computer data to an unauthorised person and, (3) the intentional and unlawful destruction or alteration of computer data that is 'required to be maintained by law or is an evidence in any proceeding under this Act.'

ARTICLE 19 makes the following observations about these provisions:

- Sections 7(1) and (2) lack any requirement that serious harm result from any illegal data interference before criminal liability attaches;[45]

- It is unclear how Section 7(1)(f) (on the obstruction, interruption or interference 'with any person in the lawful use of computer data') differs in practice from Section 7(1)(e), which criminalises the intentional and unlawful obstruction, interruption or interference with computer data. If the commission of an offence under Section 7(1)(f) requires any physical assault or coercion to take place then we believe that such an offence would be best dealt with under more relevant parts of the criminal law. If that was not the intention of the legislature, then the provision should be removed altogether as it in effect is a duplicate of Section 7(1)(e);

- Section 7(1)(g) is similarly unclear as it fails to specify that any unlawful and intentional denial of access be committed electronically or by way of interference with a computer system or network. As it stands therefore it could be interpreted as including the physical blocking of an individual from accessing computer data, which is an offence that would best be dealt with under more appropriate provisions of the criminal law dealing with assault;

- Section 7(2) fails to attach requirements for unlawfulness and intentionality in the commission of the offence. This means that this Section would allow for the prosecution of potential whistleblowers in breach of international standards on freedom of expression.[46] Furthermore, Section 7(2)(b) would also criminalise the receipt of 'unauthorised' computer

[44] *C.f.* Article 3 of the Cybercrime Convention, *op.cit.*
[45] *C.f.* Article 4(2) of the Cybercrime Convention, *op.cit.*
[46] Refer to our general comments and recommendations above for more detail

data, which without a *mens rea* of intent could potentially lead to the prosecution of individuals who even inadvertently receive 'unauthorised' computer data.

Recommendations:

- Sections 7(1) and (2) should be amended to include reference to the need for serious harm to have resulted from the commission of an offence before criminal liability attaches;
- Section 7(1)(f) should be struck out;
- Section 7(1)(g) should be amended to make specific reference to denial of access via electronic means, or physical interference with computer systems or networks; and
- Provisions requiring that the commission of an offence under Sections 7(2)(a) and (b) be done intentionally and unlawfully should be included and a public interest defence must be made available to protect whistleblowers.

Sections 8-12: Data espionage, illegal system interference, illegal device, computer-related forgery and computer-related fraud

Section 8 criminalises the obtaining of computer data, without permission, protected against unauthorised access, without prejudice to the National Security Act. The phrasing of the section is unduly vague and, as with Section 7(2), does not include any requirement of intentionality, unlawfulness or for serious harm to have resulted following the commission of an offence.

Section 9 criminalises the unlawful hindrance or interference with the functioning or usage of a computer system. The provision is unduly broad, as it does not include an intentionality requirement or a requirement that serious harm result from the commission of an offence.[47]

Section 10 criminalises the unlawful dealing in or possession of a device, including a computer program, password or access code that is designed or adapted for the purpose of committing an offence. Section 10 is overly broad and too vague in its wording as it does not specify what offences are included within its remit. Concerningly, Section 10(1)(a) does not include a requirement that any offence be committed intentionally. This is particularly concerning given that Section 10 criminalises the mere possession of a device that is capable of 'committing an offence.' When read inclusively therefore, the wording of Section 10(a) is capable of criminalising the possession of pretty much any type of computing machine or software program, as technically any computer is capable of being used to commit some form of offence should there be an *intention* to use it for such a purpose.

Section 11 criminalises intentional and unlawful computer-related forgery. We welcome the inclusion of the requirement of intentionality within this Section. However, to conform with international human rights standards, the Section should include a requirement that any intention to commit forgery be dishonest before criminal liability attaches, as suggested by Article 7 of the Cybercrime Convention.

Section 12 criminalises intentional and dishonest computer-related fraud. We welcome the inclusion of the requirement for dishonest intention before criminal liability attaches. Nonetheless, the Section could be strengthened through the inclusion of the words 'with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person' after Section 12(1)(b) in line with the wording of Article 8 of the Cybercrime Convention.

Recommendations:

- Section 8 should be redrafted to clarify in more precise terms that any 'unauthorised' access must be unlawful, intentional and result in serious harm in order for criminal liability to arise;

[47] *C.f.* Article 5 of the Cybercrime Convention, *op.cit.*

- Section 9 should be redrafted to make explicit reference to the need for intentionality and the 'serious hindering without right' of the functioning or usage of a computer system;
- Section 10 should be redrafted. At the very least, a requirement of intentionality should be included and the list of offences to which the provision applies should be explicitly set out. The title of the Section should be changed from 'illegal device' to 'misuse of devices' to reflect the fact that the mere possession of an electronic device is not an offence but rather the intention with which it is used;
- Section 11 should be amended to include a requirement for dishonest intent before criminal liability attaches; and
- The phrase, 'with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person' should be included after Section 12(1)(b).

Section 13: Child pornography

Section 13 criminalises the publication, the making available of, or facilitation of access to, child pornography. Whilst child pornography is a type of expression that States are required to prohibit under international law,[48] ARTICLE 19 notes the absence of a requirement of intentionality in the commission of the offences. Furthermore, we observe that the Section is limited in scope; for example, the intentional and unlawful production, procurement or possession of child pornography is not criminalised (or there is no reference to any legislation that could eventually criminalise these offences).

Recommendations:

- Section 13 should be amended to clarify that offences must be unlawfully committed with intent; and
- The section should also be expanded to include the unlawful and intentional production, procurement and possession of child pornography as offences, unless they are already provided for elsewhere.

Section 14: Pornography

Section 14 criminalises the publication, through a computer system or any other information and communication technology, of pornography 'or pornography that is lascivious or obscene.'

ARTICLE 19 notes that these provisions amount to legislation prohibiting "obscenity." Notwithstanding this, there is no mention of the need for intentionality and the terms pornography, lascivious and obscene are not defined within the Section or at any other part of the Act (or in other legislation). This renders the provisions unduly broad and open to subjective interpretation. ARTICLE 19 has long fought against obscenity laws, which are based on eminently subjective definitions and interpretations by governments and courts alike. Pornography is <u>not</u> one of the forms of expression that may be restricted under international law and in this regard, the HR Committee has affirmed that restrictions on freedom of expression for the protection of public morals must be based on a broad understanding of what 'public morals' means. In other words, any restriction must be founded in objective criteria not loose, subjective interpretations.

Recommendation:

- Section 14 should be struck out in its entirety.

[48] *C.f.* the May 2011 Report of the Special Rapporteur, *op.cit.*; and the Cybercrime Convention, Article 9.

Section 15: Identity related crimes

Section 15 criminalises the impersonation of another person through use of a computer system. ARTICLE 19 notes that there is no requirement that any impersonation be unlawful, be committed with dishonest intent, or that serious harm result from the commission of the offence. This means that in practice, under the current wording, legitimate and lawful forms of expression including political satire where an actor were to impersonate a public figure would be criminalised for example. At the very least, it is likely that the current wording would have a chilling effect on the right to freedom of expression and individuals may feel obliged to refrain from electronically sharing perfectly legitimate and lawful content for fear of prosecution.

Recommendation:

- Section 15 should be struck out, or at the very least amended to include a requirement that any identify related crime be committed unlawfully, with dishonest intent, and that serious harm has resulted from its commission. Furthermore, reasonableness and public interest defences should be made available.

Section 16: Publication of false information

Section 16 criminalises the publication of false, deceptive, misleading or inaccurate information.

ARTICLE 19 finds that these provisions violate international freedom of expression standards. As it stands, any Internet user who were to inadvertently share a tweet or Facebook post for example that contained false, deceptive, misleading or inaccurate information could be prosecuted under this provision. It would also make the work of online media outlets susceptible for prosecution. Although media should not aim to report false news, an actual prohibition on such news makes the work of journalists covering current developments unreasonably dangerous, as in situations of breaking news; facts are often difficult to verify. Moreover, it is often open to debate as to what the 'truth' of a particular matter is and the State should trust citizens to reach their own conclusions instead of imposing its particular view of events upon them.

We also note that the HR Committee has condemned the use of false news/information provisions in national laws, cautioning that they "unduly limit the exercise of freedom of opinion and expression." [49] It has also been clarified that the "prosecution and punishment of journalists for the crime of publication of false news merely on the ground, without more, that the news was false [is a] clear violation of Article 19 of the [ICCPR]."[50]

Recommendation:

- Section 16 should be struck out in its entirety.

Sections 17-19: Racist and xenophobic material, racist and xenophobic motivated insult, and genocide and crimes against humanity

Sections 17–19 respectively criminalise the production and distribution of racist and xenophobic material, insulting another person through a computer system on grounds of race and the unlawful publication through a computer system of material that incites acts constituting genocide or crimes against humanity.

ARTICLE 19 finds that these provisions fall short of what is required under international law. As noted above, under Article 20 para 2 of the ICCPR, states are required to "prohibit" certain forms of speech which amount to "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence."

[49] Annual General Assembly Report of the HR Committee, UN Doc. A/50/40, 3 October 1995, para.89.
[50] HR Committee, Concluding Observations on Cameroon, 4 November 1999, CCPR/C/79/Add.116.

ARTICLE 19 has developed a specific policy on prohibitions of incitement that elaborates on the interpretation of Article 20(2) of the ICCPR in a greater detail;[51] in particular, we have recommended, *inter alia*, that:

- States should adopt uniform and clear definitions of key terms within Article 20(2) of the ICCPR, including for: "hatred," "discrimination," "violence," and "hostility"[52] and make sure that interpretation is consistent within jurisprudence produced by domestic courts;

- Although Article 20(2) of the ICCPR only lists three characteristics that States are required to protect from incitement – nationality, race, and religion – the list should be read in light of Article 2(1) and Article 26 of the ICCPR, requiring States to prohibit incitement also on the basis of "sexual orientation" and "gender identity" and disability. This interpretation would comply with the evolution of developments in the protection of human rights since the adoption of the ICCPR in 1977; [53]

- The intent of the speaker to incite to hatred (that is to incite others to commit acts of discrimination, hostility or violence) should be considered a crucial and distinguishing element of incitement as prohibited by Article 20(2) of the ICCPR. Importantly, the element of intent distinguishes incitement from other forms of expression that may offend, shock or disturb but are nevertheless protected under Article 19(2) of the ICCPR. Hence, ARTICLE 19 recommends that domestic legislation should always explicitly state that the crime of incitement to hatred is an intentional crime[54] and not a crime that can be committed through recklessness or negligence.[55] The elements of intent should therefore include:
  - Volition (purposely striving) to engage in advocacy to hatred;
  - Volition (purposely striving) to target a protected group on the basis of prohibitive grounds; and
  - Having knowledge of the consequences of his/her actions and knowing that the consequences will occur or might occur in the ordinary course of events.

---

[51] ARTICLE 19, Prohibiting incitement to discrimination, hostility or violence, 2012; available at http://bit.ly/VUzEed

[52] ARTICLE 19 recommended that the definition of these terms should be as follows:

- Hatred is a state of mind characterised as "intense and irrational emotions of opprobrium, enmity and detestation towards the target group." See, Camden Principles on Freedom of Expression and Equality, ARTICLE 19, 2009.
- Discrimination shall be understood as any distinction, exclusion, restriction or preference based on race, gender, ethnicity, religion or belief, disability, age, sexual orientation, language political or other opinion, national or social origin, nationality, property, birth or other status, colour which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life. This definition is adapted from those advanced by the Convention on the Elimination of All Forms of Discrimination against Women and the Convention on the Elimination of All Forms of Racial Discrimination.
- Violence shall be understood as the intentional use of physical force or power against another person, or against a group or community that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation. The definition of violence is adapted from the definition of violence by the World Health Organisation in the report World Report on Violence and Health, 2002.
- Hostility shall be understood as a manifested action of an extreme state of mind. Although the term implies a state of mind, an action is required. Hence, hostility can be defined as the manifestation of hatred – that is the manifestation of "intense and irrational emotions of opprobrium enmity and detestation towards the target group." Camden Principles, *op. cit.*, Principle 12.1.

[53] The ICCPR was adopted before equality movements around the world made significant progress in promoting and securing human rights for all. However, it has since come to be interpreted and understood as supporting the principle of equality on a larger scale, applying to other grounds not expressly included in the treaty text, including sexual orientation, gender identity, and disability.

[54] In some jurisdictions, also acting "wilfully" or "purposefully."

[55] ARTICLE 19 notes that the legislation of many States already recognises intent or intention as one of the defining elements of incitement, for example, the UK, Ireland, Canada, Cyprus, Ireland, Malta, and Portugal.

Additionally, with a view to promoting coherent international, regional, and national jurisprudence relating to the prohibition of incitement, ARTICLE 19 proposes that all incitement cases should be assessed under a uniform incitement test, consisting of a review of all the following elements:

- Context: of the expression within broader societal context of the speech;
- Intent: of the speaker to incite to discrimination, hostility or violence;
- Position and role of the speaker: whether in a position of authority and exercising that authority;
- Content: form and subject matter of expression, tone and style;
- Extent of the expression: public nature of the expression, the means of the dissemination, magnitude of the expression; and
- Likelihood of imminent harm: probability of discrimination, hostility or violence as a result of the expression.

The provisions of Sections 17-18 do not meet these criteria for the following key reasons:

- The above provisions go beyond permitted restrictions under Article 20 (2) of the ICCPR as they are broader than the prohibition of "any *advocacy* [...] that constitutes *incitement* to discrimination, hostility or violence shall be prohibited by law." The terms "insulting" or "unlawful publication" contravene international standards;

- There is no requirement that any offence be committed intentionally. The terms "advocacy" and "incitement" imply that negligence or recklessness are not sufficient to impose sanctions and that something more than intentional distribution or circulation is required; and

- The provisions are under-inclusive in that they fail to protect against all forms of discrimination and intolerance. ARTICLE 19 advocates protection against all forms of discrimination and intolerance including on the grounds of sex, age, political or other opinion, sexual orientation, gender identity or disability. This is in line with the HR Committee's interpretation of the guarantees against discrimination contained in Article 2(1) and Article 26 of the ICCPR.[56]

The provisions prohibiting "unlawful publication" that "incites acts constituting genocide or crimes against humanity" suggest that these provisions suffer from a lack of connection with international law on the crime of genocide. From this perspective, if the provisions are intended to target any genocide-related form of expression, they should be directed at the "direct and public incitement to commit genocide" which Tanzania is required to prevent and punish as a state party to the Genocide Convention.[57] Moreover, there is no requirement under Section 19 that any incitement to commit genocide be direct, public and committed with specific intent, as is required under international law.

Further, it is unclear whether provisions criminalising racist and xenophobic material and the incitement to genocide and crimes against humanity exist in other parts of Tanzania's criminal law. If alternative provisions do exist, then the inclusion of Sections 17-19 might undermine the principle of equality before the law as they treat individuals committing the same offence differently only by reference to whether or not they have used a computer. To the extent that racist and xenophobic speech that amounts to incitement under Article 20 para 2 and material, and direct and public incitement to commit genocide remain outside the scope of existing criminal

[56] On sexual orientation see: HR Committee *Toonen v Australia*, Comm. No. 488/199, CCPR/C/50/D/488/1992, on disability see HR Committee, General Comment no. 25 of 1996 on the right to take part in the conduct of public affairs, the right to vote and to be elected, and the right to equal access to public services (Article 25) at para.10 and Concluding Observations on Ireland, 24 July 2000, A/55/40, paras 422-451, at para.29 (e).
[57] The Convention on the Prevention and Punishment of the Crime of Genocide of 1948, Article III(c),

law, then these issues should be addressed there by amending existing legislation rather than creating separate offences under the Act.

Recommendations:

- Sections 17-19 should be removed from the Act and the offences they establish should be clearly set out in more appropriate parts of the criminal law taking into account the above guidance.

Section 20: Unsolicited messages

Section 20 criminalises the initiation, transmission, relay, retransmission and falsification of headers of unsolicited messages.

ARTICLE 19 observes that the wording of this section is vague, which severely compromises the principle of legal certainty and criminalises the sending of any 'electronic message' to another person without their knowledge. This provision has the potential to have significant and unpredictable implications on basic personal and commercial communication practices. If it is the intention of the legislature to target unlawful and intentional spamming and phishing practices then we recommend that the section be entirely re-written with explicit, sufficiently clear and precise reference to the practices which are being criminalised and the conditions that must apply before criminal liability attaches. Furthermore, definitions for any practices that the legislature seeks to criminalise should be included under Section 3 of the Act.

Outside of the context of spamming and phishing, in any non-commercial sense, malicious unsolicited messages can be dealt with adequately under harassment provisions within Tanzanian criminal law. To the extent that they are not, we recommend that the relevant criminal laws be amended to include them and that the provision be struck out or amended to clarify that it does not apply to non-commercial correspondence. Furthermore, a public interest defence or a defence of reasonableness should be provided for. The absence of any such defences significantly heightens the risk that the section could be applied arbitrarily and unpredictably, and could therefore be used to punish individuals engaged in entirely legitimate activities.

Recommendation:

- Section 20 in its current form should be struck out.

Sections 21-22: Disclosure of details of investigation and obstruction of investigation

Section 21 criminalises the disclosure of details of a confidential criminal investigation and Section 22 the obstruction of investigations through the intentional and unlawful destruction, deletion, alteration, concealment, modification or rendering of computer data meaningless, ineffective or useless. ARTICLE 19 believes that these provisions do not belong in this Part of the Act and they would be best placed within Tanzanian criminal procedure law, or at least under a 'Procedural Law' Part within the Act.

Recommendation:

- Section 20 should either be removed entirely from the Act or moved to a new Part on Procedural Law (as per above).

Section 23: Cyber bullying

The provision criminalises the initiation or sending of any electronic communication using a computer system with the intent to coerce, intimidate, harass or cause emotional distress to that person.

ARTICLE 19 notes that whilst the right to privacy requires that the criminal law protect individuals from harassment, threats and other forms of intimidation, we do not recommend that provisions designed to protect individuals from intimidation and harassment separate to those that exist in other parts of Tanzanian criminal law be repeated here. To the extent that Tanzanian law fails to provide sufficient protection in this area, the Tanzanian legislature should take immediate steps to ensure that the criminal law is adequate for this purpose.

Notwithstanding these remarks, the provisions as they stand are both inadequate in terms of their protective scope and also fail to provide adequate safeguards against misapplication. In particular:

- It is unclear why the scope of the offence is limited to using a "computer system" with the intent to coerce, intimidate, harass or cause emotional distress to another person. Such conduct would be equally criminal regardless of the mode of its transmission; and
- Core terms including 'coerce', 'intimidate', 'harass' and 'emotional distress' are not defined in the Act, nor are there provisions referring to other Acts in which the terms are defined. As a result we believe that there is too broad a scope for misapplication of the provisions to target legitimate forms of expression, particularly in the context of legitimate protests and investigative journalism. These concerns are compounded by the lack of any defence of reasonableness or public interest.

Recommendation:

- Section 23 should be struck out. Legislation against harassment, coercion and intimidation should be dealt with under broader criminal law, containing clearly defined terms to ensure that the provisions are lawful and that clearly defined public interest and reasonableness defences are available to protect legitimate forms of freedom of expression.

Section 24: Violation of intellectual property rights

Section 24 of the Act criminalises the use of a computer system to violate intellectual property rights protected under 'any written law'.

ARTICLE 19 finds these provisions problematic for the following key reasons:

- The provisions are overbroad and unduly vague; they have a potential to criminalise Internet users for largely innocuous and non-commercial acts of copyright infringement.

- The necessity or proportionality of criminalising intellectual property rights infringements in this manner is also entirely unclear. It appears that criminal charges may be brought even where no harm has been caused to the rights holder or without even a requirement that the rights holder file a complaint for a prosecution to be initiated. It is not clear what the necessity of using the criminal law when no harm to an individual has been proven is. One may argue that the advantage to the user in accessing material protected by intellectual property results in a corresponding economic loss to the copyright holder; for example, through lost sales. Such an assertion can only ever be speculative, and discounts the possible economic benefits that a secondary market in electronic data may have for a copyright holder. In any event, the Section does not require the need to entertain this evaluation, as the infringement itself is a criminal offence irrespective of the impact on the copyright holder.

ARTICLE 19 has long argued that criminal sanctions for non-commercial copyright infringement have a chilling effect on the free flow of information and ideas and as such are a disproportionate interference with the right to freedom of expression. They should be abolished in their entirety and replaced by civil remedies where appropriate.[58]

[58] *C.f.* ARTICLE 19, The Right to Share: Principles on Freedom of Expression and Copyright, 2013.on Freedom of Expression and Copyright in the Digital Age, London, 2013.

Furthermore, in respect of commercial infringements (Section 24(1)(b)), we note that the lack of clarity and overbroad wording of the provision may lead to malicious requests between commercial competitors for the prosecution of alleged infringements when such disputes would be better resolved in the civil courts.

Recommendations:
- Non-commercial infringements of intellectual property rights should be abolished; and
- In relation to commercial offences, Section 24 should be revised, taking into account the above guidance.

Sections 25-27: Principle offenders, attempt and conspiracy to commit offence
Sections 25-27 of the Act deal with the commission of offences by principle offenders, aiding and abetting and conspiracy to commit any offence under the Act.

Notwithstanding our general recommendation regarding the sanctions regime under the Act, ARTICLE 19 observes the absence of a requirement for intent within Sections 25 and 27. Furthermore, it is unclear why three separate sections have been drafted and would recommend that they be merged into one clearer provision.[59]

Recommendation:
- Sections 25-27 should be merged and rephrased; and, a *mens rea* requirement of intentionality should be included for the offences set out in Sections 25 and 27.

Sections 28 and 29: Protection of critical information infrastructure and offences relating to critical information infrastructure
Sections 28 and 29 relate to the protection of critical information infrastructure and offences relating to critical information infrastructure.

Whilst ARTICLE 19 does not have any specific concerns relating to the content of the provisions, in relation to Section 29 in particular, we recommend that this be listed as an aggravating factor for the purposes of the imposition of sanctions, as opposed to a separate provision under the Act - further to our general recommendation that the sanctions regime under the Act be entirely re-drafted.

Recommendation:
- Section 29 should be struck out and instead be listed as an aggravating factor under a sanctions Section/Part.

Sections 31-38:
Sections 31-38 of the Act respectively cover: search and seizure, disclosure of data, expedited preservation, the disclosure and collection of traffic data, the disclosure and collection of content data, court orders, the use of forensic tools and application hearings.

Firstly, we would reiterate the lack of procedural safeguards within the Act as a whole, particularly the absence of any reference to Tanzania's international obligations to uphold and protect the right to freedom of expression and the right to privacy. Furthermore, the absence of judicial oversight of the broad powers contained within Part IV of the Act is concerning, particularly the absence of a

[59] *C.f.* Cybercrime Convetion, Article 10.

requirement for a court order to be obtained prior to the execution of search and seizure powers (as per Section 31 of the Act).

Moreover, the powers set out in Sections 31-38 appear to apply to the commission of any of the offences listed within the Act, without any regard to the seriousness of the alleged offence. This is a disproportionate set of intrusive powers in the absence of any available defences or channels to challenge the execution of the powers set out within the Part. As a result, ARTICLE 19 has a series of recommendations relating to Part IV, which should be read alongside our general recommendations as set out above.

Recommendations:

- To clarify the limitations of police powers under Part IV of the Act, all references to the word 'may' in relation to the discretion of police officers to apply to the court for an order permitting them to execute their powers under Part IV should be replaced with the word 'must' to secure adequate judicial oversight. Specifically, the word 'may' should be replaced with the word 'must' within Sections 32(3), 33(2), 36 and 37(1);
- Within Section 36, the specification that a police officer 'may' apply to the court for an order only in instances where his powers cannot be executed without the threat of the use of force should be removed entirely and replaced with a specific requirement that a police officer in charge of a police station must apply to the court for order for the execution of <u>any</u> of his powers under Section 36 and Part IV more broadly;
- Furthermore, all applications for court orders for the execution of powers set out within Part IV must be supported by grounds showing reasonable suspicion or probable cause;
- Moreover, where it is deemed appropriate by a court of law following consideration of an application that meets the above requirements, a suspect must be offered the right to challenge the application; and
- Finally, Part IV should be amended to specify that powers within Part IV should only be applied in relation to specified serious offences.

Sections 39–44: Liability of ISPs

Sections 39–44 set out provisions relating to the liability of service providers. They respectively cover monitoring obligations; the provision of access, hosting, caching, and hyperlinking services, and the services of search engine providers.

ARTICLE 19 has long argued that in order to comply with international standards on freedom of expression, hosts should in principle be immune from liability for third-party content in circumstances where they have not been involved in modifying that content.[60] Also, states should not delegate censorship measures to intermediaries. Hosts should only be required to remove content following an order issued by an independent and impartial court or other adjudicatory body that has determined that the material at issue is unlawful. Moreover, from the perspective of hosts, orders issued by independent and impartial bodies provide a much greater degree of legal certainty.

Whilst ARTICLE 19 commends the opening provisions of Section 39 that clarify that service providers shall not be obliged to monitor the data which they transmit or store. Nonetheless, we make several observations about these provisions:

- At Section 39(2), power is conferred upon the Minister to prescribe procedures for service providers. However, there is no requirement that these procedures be proactively published and placed into the public domain for the public to access. International standards on freedom of information require that any such procedures be publically published.

[60] ARTICLE 19, Intermediaries: Dilemma of Liability, 2013.

- Section 39(3) places an evidential burden upon the service provider to prove that they are not liable for third party disclosure. This runs contrary to international standards in this area, which clearly stipulate that intermediaries should be fully insulated from liability for content generated by others. Within the context of the criminal law, where an allegation against an intermediary as to their collusion in the illegal disclosure of data is made as part of a prosecution, it should be for the prosecution to prove beyond reasonable doubt that the intermediary was involved.

- Section 39(4) confers power upon a service provider to remove information, terminate or suspend services and notify appropriate law enforcement agencies of any alleged illegal activity. In its current form, this provision places the onus upon the service provider to determine what may or may not be illegal activity.

- It is unclear what Sections 40 and 44 add to Section 39.

- In relation to Sections 41-43 covering hosting providers, caching providers, and hyperlink providers it is unclear why these are separate sections when the provisions they contain are remarkably similar. Similarly to our concerns regarding the undue powers conferred upon intermediaries, we note that the powers that have been conferred upon access, hosting, caching and hyperlink providers to remove information after receiving an order from 'any competent/relevant authority' are too broad and ill-defined. Competent authorities are not defined under Section 3 of the Act and no consideration has been given to the provision of legitimate defences.

Recommendations:
- Section 39(2) should be amended to clarify that any procedures that are developed should be proactively published;
- The burden of proof set out at Section 39(3) should be reversed and it should be for the prosecution to prove beyond reasonable doubt, on a case-by-case basis, that an intermediary illegally disclosed data;
- Section 39(4) should be struck out;
- Section 40 should be struck out;
- All references to 'competent/relevant authorities' should be removed (from Sections 41(1)(a), 42(e) and 43(a)). The terms should be replaced with a provision that makes clear that information shall only be removed by providers upon receipt of a court order, which has been made following an application made to the court setting out grounds showing reasonable suspicion or probable cause that a serious specified crime has been committed. Furthermore, where appropriate, as decided by a court of law, a suspect shall have the right to hear the application against him and file a defence.

Section 45: Take-down notification

Section 45 confers power upon a service provider to take down content following its reporting by 'a person' subject to the conditions set out at Sections 45(2) being met. Section 45(4) states that a service provider shall not be held liable for a take down done in compliance with a notification under the Act.

ARTICLE 19 proposes that the notice and take down regime be abolished. Alternatively, we recommend that notice-to-notice procedures should be developed instead. These would allow aggrieved parties to send a notice of complaint to the host. In order to comply with international standards and best practice, notice-to-notice systems should meet the following conditions:

- The notice sent by an aggrieved party should include minimum requirements, including: the name of the complainant, the statement concerned with an explanation as to why it should be considered unlawful, including the provision of a legal basis for the claim, the location of the material; and, an indication of the time and date when the alleged wrongdoing was committed. If the notice complies with these requirements, and upon payment of a fee, the host will then be required to forward the notice electronically as soon as is practicable (e.g. within 72 hours) to the person identified as the wrongdoer. They could be identified either directly by the complainant or via their IP address. The claimant will then be informed that the notice had been forwarded or, if not, why this was not possible.

- The alleged wrongdoer will then have a choice of either removing the content and informing the complainant (directly or via the host) or of filing a counter-notice within a sufficient time period (e.g. 14 days of receipt of the notice). The host will then forward the counter-notice within a set time (e.g. 72 hours) to the complainant, who will have another period of time (e.g. 14 days upon receipt of the counter-notice) to decide whether or not to take the matter to a court or other independent body with adjudicatory powers to determine the matter. Depending on the content at issue and the complexity of the complaint, consideration will be given to fast-track and low-cost procedures.

- If the alleged wrongdoer wishes to remain anonymous and refuses to give their contact details when filing the counter-notice, the complainant would have to seek a disclosure order from the court in order to bring the matter before the courts. This would at least stem the tide of abusive claims by adding the additional hurdle of convincing a court that disclosure was necessary. In this scenario, the only remedy available to claimants against online service providers would be statutory damages for failing to comply with their 'notice-to-notice' obligations.

- If the alleged wrongdoer fails to respond or file a counter-notice within the required time limit, the host will lose its immunity from liability. In other words, the host will have a choice. It can either take the material down or decide not to remove it, in which case it may be held liable for the content at issue if the complainant wishes to take the matter to a court or other independent adjudicatory body.

ARTICLE 19 believes that this system would work well when dealing with civil claims relating to copyright, defamation, privacy, adult content and bullying (as opposed to harassment or threats of violence). In our view, such a system would at the very least give content providers the opportunity to respond to allegations of unlawfulness before any action was taken; it would contribute to reducing the number of abusive requests by requiring a minimum of information about the allegations; and, it would provide an intermediate system for resolving disputes before matters were taken to court. In this respect, we are concerned at the absence of judicial oversight of this process in the Act.

Recommendations:

- The notice and take down regime should be abolished. As an alternative, a notice-to-notice regime could be established, based on the above guidance.

Section 49: Offence by corporate body

Section 49 sets out provisions relating to the commission of an offence by a corporate body.

ARTICLE 19 notes that this Section has a very broad scope that includes 'every' person who, at the time of the commission of the offence was a director, officer or is otherwise concerned with the management of the corporate body. Moreover, the Section reverses the evidential burden of

proof, placing the emphasis on the accused to show that any alleged offence took place without their consent and that they exercised due diligence to prevent the commission of the offence.

Moreover, the wording of the Section is insufficiently clear and does not enable an accused individual to regulate their conduct accordingly. For example, it is unclear what the evidential measure on which an accused would have to 'prove' that they did not consent and did exercise due diligence is – the balance of probabilities or beyond reasonable doubt.

Recommendations:

- Section 49 should be amended, specifically so that no person shall be held liable unless there is clear evidence of illegal conduct against them; and
- The evidential burden of proving illegal conduct should be reversed to lie with the prosecution to prove beyond reasonable doubt that an offence was committed.

About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, 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 the ARTICLE 19's work in East Africa, please contact Henry Maina, Director of ARTICLE 19 Kenya and East Africa, at henry@article19.org.

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