Kenya: Information Communications (Cybersecurity) and (Electronic Transactions) Draft Regulations

April 2016

Legal analysis

Executive summary

In this analysis, ARTICLE 19 reviews the draft Information Communications (Cyber-security) Regulations 2016 and the Information Communications (Electronic Transactions) Regulations 2016, published in December 2015 by the Kenyan Communications Authority. The power to make these regulations comes from the Kenya Information and Communications Act (KICA), 1998 as amended. The regulations have been subject to public consultations in April 2016.

ARTICLE 19 notes at the outset that the Cyber-security Regulations and the Electronic Transactions Regulations create a number of Internet-specific offences and substantive regulatory obligations for Internet intermediaries and telecommunications providers. In our view, however, the development of substantive law provisions through regulations, which are subject to much less public scrutiny and debate than parliamentary bills, is deeply problematic. It is particularly inappropriate in circumstances where the regulations purport to create new serious offences. In our view, mere reference to the licensing and registration provisions of KICA is insufficient to justify the adoption of these regulations, which have serious implications for the rights to freedom of expression and privacy. We also seriously question whether KICA provides any kind of basis for the procedures and powers laid down in the Kenya Information Communications (Cyber-security) Regulations 2016 ('Cybersecurity Regulations') and the Kenya Information Communications (Electronic Transactions) Regulations 2016 ('Electronic Transactions Regulations').

Notwithstanding these concerns, this legal analysis reviews the compatibility of the regulations with international standards on freedom of expression. We merely highlight areas of concern.

We conclude that several speech offences created by the Cybersecurity Regulations must be withdrawn as they unduly restrict legitimate expression, in breach of international standards on freedom of expression. Similarly, the various obligations imposed on cyber-cafes and operators of wireless hotspots, such as mandatory SIM-card registration as a pre-condition for access to online services etc. and broad data retention requirements, are incompatible with international standards for the protection of the rights to freedom of expression and privacy. As such they should be removed from the Cybersecurity Regulations. Similar considerations apply to data localisation requirements.

Several provisions of the Electronic Transactions Regulations are equally problematic. The Regulations require providers of good and services online to obtain an authorisation from the Authority in breach of international standards on freedom of expression and, for all intents and purposes, *ultra vires* the authorising statute. While the service providers liability provisions contain some positive elements, they could still be further improved as detailed in our recommendations. The sanctions provisions remain problematic as being both disproportionate and lacking a proper basis in statute.

Summary of recommendations:

1. The Cyber-Security Regulations and Electronic Transactions Regulations should be scrapped and replaced with Parliamentary Bills instead;
2. Any statute creating new offences of child pornography should provide a definition of 'child pornography' in line with the definition of the COE Cybercrime Convention or African Union Convention on Cybersecurity and Personal Data Protection;
3. Clause 6 (d) to (h) of the Cybersecurity Regulations should be removed;
4. Provisions equivalent to Clause 6 (d), (e), (g) and (h) of the Cybersecurity Regulations should be repealed from the relevant statutes;

5. The prohibition of incitement to genocide and of the advocacy of hatred that constitutes incitement to violence, hostility or discrimination should be consistent with international standards on freedom of expression;
6. Clause 7 of the Cybersecurity Regulations on the obligations of operators of cybercafés and public wireless hotspots should be removed;
7. Clause 10 (1) of the Cybersecurity Regulations on data localisation requirements should be removed;
8. Clause 4 of the Electronic Transactions Regulations should be removed: service providers should not be subject to an authorisation process;
9. Clause 12 should be removed. Information location service providers should benefit from the same immunity from liability as other service providers. At a minimum, clause 12 should be amended as follows: (1) 'infringing' should be replaced with "unlawful"; clause 12 (b) to (d) should be removed; clause 12 (a) should specify that actual knowledge can only be obtained by a court order;
10. Clauses 13 and 14 should be removed. User data should only be disclosed by a court order. Provision for such disclosure should be laid down in statute rather than regulations. At a minimum, it should be set out in detail in legal instruments rather than guidelines.
11. Clause 15 should be removed as overly broad.
12. KICA should be amended so that network service providers are no longer required to obtain a licence. This would make Clause 11 (2) (b) redundant.
13. Failure to comply with the regulations should not be meted out with criminal penalties, let alone imprisonment. At a minimum, Clause 16 should be re-drafted to align with the relevant section of KICA.

Introduction

In December 2015, the Communications Authority published several regulations for public consultation on their website, including the Kenya Information Communications (Cyber-security) Regulations 2016 and the Kenya Information Communications (Electronic Transactions) Regulations 2016. The power to make these regulations comes from the Kenya Information and Communications Act (KICA), 1998 as amended. On April 18, 2016 the Communications Authority held public consultations on these regulations and announced that the deadline for submission of memoranda would April 21, 2016.

ARTICLE 19 notes at the outset that the Cyber-security Regulations and the Electronic Transactions Regulations create a number of Internet-specific offences and substantive regulatory obligations for Internet intermediaries and telecommunications providers. In our view, however, the development of substantive law provisions through regulations, which are subject to much less public scrutiny and debate than parliamentary bills, is deeply problematic. The purpose of regulations is to give effect to the provisions and principles laid down in statute, not to lay down substantive principles themselves. It is therefore particularly inappropriate for the regulations to create new serious offences. In our view, mere reference to the licensing and registration provisions of KICA is insufficient to justify the adoption of regulations, which have serious implications for the rights to freedom of expression and privacy. We also seriously question whether KICA provides any kind of basis for the procedures and powers laid down in both regulations.

This analysis suggests how both Regulations should be revised to fully comply with international human rights standards on the right to freedom of expression.

International standards on freedom of expression

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, including Article 19 of the Universal Declaration on Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR). The UDHR, as a UN General Assembly Resolution, is not directly binding on states. However, parts of it, including Article 19, are widely regarded as having acquired legal force as customary international law since its adoption in 1948. Kenya further acceded to the ICCPR on 1 May 1972 and is therefore legally bound to respect and to ensure the right to freedom of expression as contained in Article 19 of the ICCPR.

Kenya also ratified the African Charter on Human and **Peoples' Rights 1983** (ACHPR), which guarantees the right to freedom of expression in Article 9. 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.

In September 2011, the UN Human Rights Committee ('HRC'), as treaty monitoring body for the ICCPR, issued General Comment No 34 in relation to Article 19.[1] General Comment No.34 constitutes an authoritative interpretation of the minimum standards guaranteed by Article 19 ICCPR.[2] General Comment No 34 states 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.[3] In other words, the protection of freedom of expression applies online in the same way as it applies offline.

At the same time, General Comment No 34 requires States party to the ICCPR 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.[4] In particular, 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.[5]

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.[6] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material

[1] See, CCPR/C/GC/3 available at http://www2.ohchr.org/english/bodies/hrc/comments.htm.
[2] ARTICLE 19 statement on UN Human Rights Committee Comment No.34; http://bit.ly/1SJhjPi.
[3] *Ibid.*, para. 12.
[4] *Ibid.*, para. 17.
[5] *Ibid.*, para. 39.
[6] See Joint Declaration on Freedom of Expression and the Internet, June 2011, http://bit.ly/1OrMt0R.

disseminated over the Internet are unnecessary.[7] They also promote the use of self-regulation as an effective tool in redressing harmful speech.[8]

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.

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:

- be provided by law, i.e. formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly;[9]
- pursue a legitimate aim as exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR; and
- conform to the strict tests of necessity and proportionality, i.e. if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.[10]

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.[11]

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[12]

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 dated 16 May 2011[13] and 10 August 2011.[14] In the latter, the Special Rapporteur also clarified the scope of legitimate restrictions on different types of expression online.[15] The UN

---

[7] *Ibid*.
[8] *Ibid*.
[9] *Leonardus J.M. de Groot v. The Netherlands*, No. 578/1994, U.N. Doc. CCPR/C/54/D/578/1994 (1995).
[10] *Velichkin v. Belarus*, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).
[11] General Comment 34, op.cit., para 43.
[12] Concluding observations on the Syrian Arab Republic (CCPR/CO/84/SYR).
[13] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27, http://bit.ly/QD35W5.
[14] UN Special Rapporteur on Freedom of Expression, A/66/290, 10 August 2011, para. 16; http://bit.ly/1tsKU8X.
[15] *Ibid*., para.18.

Special Rapporteur identified three different types of expression for the purposes of online regulation:

(i) expression that constitutes an offence under international law and can be prosecuted criminally;
(ii) expression that is not criminally punishable but may justify a restriction and a civil suit; and
(iii) expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[16]

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. [17] 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 Special Rapporteur also highlighted his concern that a large number of domestic provisions seeking to outlaw hate speech are unduly vague, in breach of international standards for the protection of freedom of expression. This includes expressions such as combating "incitement to religious unrest", "promoting division between religious believers and non-believers", "defamation of religion", "inciting to violation", "instigating hatred and disrespect against the ruling regime", "inciting subversion of state power" and "offences that damage public tranquility."

Role of Internet intermediaries and intermediary liability

Intermediaries, such as Internet Service Providers (ISPs), search engines, social media platforms and web hosts, play a crucial role in relation to access to the Internet and transmission of third party content. They have come to be seen as the gateways to the Internet.

In many western countries, Internet intermediaries have been granted complete or conditional immunity for third-party content.[18] They have also been exempted from monitoring content.[19] However, the flipside of conditional liability regimes is that Internet intermediaries are made subject to 'notice-and-takedown' procedures, whereby they are given an incentive to remove allegedly unlawful content upon notice by private parties or law enforcement agencies lest they face liability.

---

[16] *Ibid.*
[17] *Ibid,* para. 22
[18] See for example, the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, the 'E-commerce directive' in the EU. See also the Communications Decency Act 1996 in the US, and in Singapore, the Electronic Transaction Act 2010 which gives strong protection to innocent providers.
[19] See Article 15 of the E-commerce directive. In the recent case of *SABAM v. Scarlet Extended SA,* the Court of Justice of the European Union (CJEU) considered that an injunction requiring an ISP to install a filtering system to make it absolutely impossible for its customers to send or receive files containing musical works using peer-to-peer software without the permission of the rights holders would oblige it to actively monitor all the data relating to each of its customers, which would be in breach of the right to privacy and the right to freedom to receive or impart information. The court noted that such an injunction could potentially undermine freedom of information since the suggested filtering system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.

Notice and takedown procedures have been sharply criticised by the UN Special rapporteur on freedom of expression, including for their lack of clear legal basis [20] and basic fairness. In particular, he noted:[21]

> 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; [22]
>
> (ii) Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;[23]
>
> (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.[24]

The protection of the right to privacy

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 right of private communications is strongly protected in international law through Article 17 of the ICCPR, which provides, *inter alia,* that

> 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.

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 of the Covenant.

[20] OSCE report, Freedom of Expression and the Internet, July 2011, p 30.
[21] See UN Special Rapporteur on Freedom of Expression report, *op.cit,* para. 42.
[22] *Supra note* 17.
[23] *Ibid.*
[24] *Ibid.*

The Committee went on to explain that the expression "arbitrary interference" was intended to guarantee that

> Even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.

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: [25]

The lack of ability of individuals to communicate privately substantially affects their freedom of expression rights. In his report of 16 May 2011, the UN Special Rapporteur on Freedom of Opinion and Expression expressed his concerns that:

> 53. [T]he Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a violation of the Internet users' right to privacy, and, by undermining people's confidence and security on the Internet, impede the free flow of information and ideas online.

In particular, the Special Rapporteur recommended that States should ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems.[26]

The protection of anonymity online

In May 2015, the Special Rapporteur on FOE published his annual report on encryption and anonymity in the digital age. The report highlighted the following issues in particular:

- The Special Rapporteur made it clear that an open and secure internet should be counted among the leading prerequisites for the enjoyment of freedom of expression today, and must therefore be protected by governments. Encryption and anonymity must be strongly protected and promoted because they provide the privacy and security necessary for the meaningful exercise of the right to freedom of expression and opinion in the digital age;[27]

- The Special Rapporteur highlighted that anonymous speech is necessary for human rights defenders, journalists, and protestors. He noted that any attempt to ban or intercept anonymous communications during protests was an unjustified restriction to the right to freedom of peaceful assembly under the UDHR and the ICCPR.[28] He also recommended that legislation and regulations protecting human rights defenders and journalists should include provisions that enable access to and provide support for using technologies that would secure their communications;

- He also stressed that restrictions to encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law. The Special

[25] 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.
[26] *Ibid.*, para 84.
[27] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 29 May 2015 (the 2015 Report of the SR on FOE), paras 12,16 and 56.
[28] *Ibid.,* para 53.

Rapporteur recommended that draft laws and policies providing for restrictions to encryption or anonymity should be subject to public comment and only be adopted following a regular – rather than fast-track – legislative process. He also emphasised that strong procedural and judicial safeguards should be applied to guarantee the right to due process of any individual whose use of encryption or anonymity is subject to restriction;[29]

- The Special Rapporteur stated that blanket bans on the individual use of encryption technology disproportionately restrict the right to freedom of expression. He also noted that rules (a) requiring licenses for encryption use; (b) setting weak technical standards for encryption; and (c) controlling the import and export of encryption tools were tantamount to a blanket ban and therefore a disproportionate restriction to freedom of expression;[30]

- The Special Rapporteur also noted that governments' backdoor access to people's communications, key escrow systems (allowing potential third-party access to encryption keys), and the intentional weakening of encryption standards are disproportionate restrictions to the rights to freedom of expression and privacy. In particular, he highlighted that governments proposing backdoor access had not demonstrated that criminal or terrorist use of encryption serves as an insurmountable obstacle to law enforcement objectives. Under international law, states were required to demonstrate, publicly and transparently, that other less intrusive means (such as wiretaps, physical surveillance and many others) were unavailable or had failed, and that only broadly intrusive measures, such as backdoors, would achieve the legitimate aim. Key escrow systems were also a threat to the secure exercise of the right to freedom of expression because of the vulnerabilities inherent in third parties being trusted to keep encryption keys secure, or being required to hand them over to others;[31]

- The Special Rapporteur also found that blanket prohibitions on anonymity online and compulsory real-name or SIM card registration go well beyond what is permissible under international law; on the contrary, he noted that because anonymity facilitates opinion and expression in significant ways online, states should protect it and, in general, not restrict the technologies that make it possible.[32]

- The report further acknowledges the role of corporate actors in protecting and promoting strong encryption standards. In particular, companies are invited to consider how their own policies restrict encryption and anonymity.

The findings of this report confirmed the earlier findings of the 2013 report of the Special Rapporteur on FOE, which observed that restrictions to anonymity facilitate states' communications surveillance and have a chilling effect on the free expression of information and ideas.[33]

Cybercrime

The Council of Europe Convention on Cybercrime CETS No. 185 (also known as the Budapest Convention) is the main binding international instrument in this area.[34] It was adopted in 2001 and has been ratified by 42 countries, including the United States, Australia and Panama, and

[29] *Ibid.,* paras 31-35.
[30] *Ibid.,* paras 40-41.
[31] *Ibid.,* paras 36, 42-44.
[32] *Ibid.,* paras 49-51.
[33] *Ibid.,* paras 48-49.
[34] The Convention is available here: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

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.

Cyber security regulations

Content-related offences

Child pornography and related offences

ARTICLE 19 notes that clause 6 provides for content-related offences, which replicate the exact wording of section 3 of the African Union Convention on Cybercrime and Data Protection. In particular, clause 6 (a) to (c) provide for various offences related to child pornography. While these provisions are broadly consistent with international practice and conventions in this area, the Cyber-security Regulations fail to define 'child pornography'. We would therefore recommend that any statute creating new offences of child pornography should provide a definition of 'child pornography' in line with the definition of the COE Cybercrime Convention or African Union Convention on Cybersecurity and Personal Data Protection.

ARTICLE 19 further notes that clause 6 (d) creates an offence of "facilitating or providing access to images, documents, sound or representation of a pornographic nature to a minor". In our view, this provision is an unjustified restriction on freedom of expression for a number of reasons.

- First, it criminalises the provision of access to material, which should be considered lawful under Kenyan law. In particular, 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.

- Secondly, it potentially criminalises parents for inadvertently allowing their children to gain access to such material on the Internet. In other words, simply by virtue of having an Internet connection at home, parents could be held criminally liable in circumstances where they failed to install pornography filters at home or failed to closely monitor the online activities of their children. This would clearly put a disproportionate burden on parents and would be deeply misguided as a matter of policy.

- Thirdly, this provision could criminalise Internet Service Providers in circumstances where they provide access to the Internet without filtering pornographic content. Put it another way, this provision effectively requires ISPs to monitor pornographic content, i.e. content which should be considered lawful, lest they face criminal liability. This is wholly inconsistent with international standards on freedom of expression, which provide that Internet intermediaries should not be held liable for content produced by others (see section on international standards on freedom of expression for more details).

Speech offences

Clause 6 (e) to (h) provide for several speech offences committed through a computer system, including:

- Creating, downloading, disseminating or making available ideas or theories of racist or xenophobic ideas or information in any forms (Clause 6 (e));
- Threatening to commit a criminal offence against a person or group of person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion (Clause 6 (f));

- Insulting to commit a criminal offence against a person or group of person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion (Clause 6 (g));
- Deliberately denying, approving or justifying acts constituting genocide or crimes against humanity.

In ARTICLE 19's view, however, the speech offences contained in section 6 (d) to (h) fall outside the scope of permitted restrictions on freedom of expression under international law. In particular, we note that the only types of expression that States are required to prohibit under international law are child pornography, direct and public incitement to commit genocide, the advocacy of hatred that constitutes incitement to discrimination, hostility or violence and incitement to terrorism. [35] For these and other restrictions on freedom of expression to be justified under international law, they must comply with the requirements of Article 19 (3) ICCPR. In particular, they must be provided by law with a sufficient degree of clarity and precision as to enable individuals to understand the foreseeable consequences of their conduct (legality test). They must also be proportionate to the purpose they seek to achieve (proportionality test). However, the offences laid down in clause (e) to (g) fail to meet these tests:

- Clause 6 (e) criminalises the mere sharing or downloading of racist or xenophobic ideas online without any requirement of intent to incite to discrimination, hostility or violence. In other words, it criminalises individuals who express racist opinions. This goes far beyond the requirements of Article 20 (2) and would criminalise expression, which whilst contemptible, should be considered legitimate.

- Clause 6 (f) criminalises the making of threats to commit crimes against individuals or groups simply for the reason that they belong to a group distinguished by race, ethnicity as well as a range of other well-established discriminatory factors (i.e. hate crimes). However, it is highly unclear that an internet-specific offence is required to deal with this type of behaviour.

- Clause 6 (g) seems to criminalise racist insults though the wording of this provision is unclear. In particular, while we understand the concept of 'threatening to commit an offence', we don't think that 'insulting to commit an offence' is capable of legal meaning. In any event, whilst racist insults may constitute incitement to discrimination in certain circumstances, particularly when uttered in the presence of others, merely 'insulting' someone, including with 'racist overtones, without any intent to incite discrimination or violence, should not be criminalised per se a disproportionate restriction on freedom of expression.

- Clause 6 (h) criminalises the denial or glorification of acts of genocide. It therefore goes beyond the requirement to prohibit incitement to genocide. As the UN Special Rapporteur on freedom of expression has noted on multiple occasions, terms like 'glorification' or 'justification' or 'approval' are too vague and serve to create overbroad offences that criminalise legitimate expression.

More generally, we note that governments should refrain from adopting new offences specifically for the Internet in circumstances where such offences may already exist on the statute book: first, such offences are generally unnecessary as they already exist; secondly, they usually lead to greater legal uncertainty which is undesirable; thirdly, they are often meted out with harsher penalties, which is inconsistent with the principle that the same behaviour should be treated the same online as offline.

[35] May 2011 Report of Special Rapporteur on FOE, *op.cit.*

Recommendations:

- Any statute creating new offences of child pornography should provide a definition of 'child pornography' in line with the definition of the COE Cybercrime Convention or African Union Convention on Cybersecurity and Personal Data Protection.
- Clause 6 (d) to (h) should be removed.
- Provisions equivalent to Clause 6 (d), (e), (g) and (h) should be repealed from the relevant statutes.
- The prohibition of incitement to genocide and of the advocacy of hatred that constitutes incitement to violence, hostility or discrimination should be consistent with international standards on freedom of expression.

Obligations of cybercafés and operators of public wireless hotspots

Clause 7 requires cybercafés and operators of public wireless hotspots to: (a) identify users before providing them with their services; (b) register users with their mobile numbers, (c) make this "information available to the authority for further action, as and when deemed necessary"; (d) maintain a register of their clients (e) install CCTV cameras "to record the identity of [their] clients"; (f) retain communication logs for no less than a year and (g) to report any cyber-crime 'incidents' within 24 hours to the authorities, among other requirements.

In ARTICLE19's view, this is plainly in breach of international standards on the rights to freedom of expression and privacy and best practice in this area:

- The UN Special Rapporteur on freedom of expression, noted in his June 2015 report on encryption and anonymity that mandatory SIM-card registration, real-name registration and broad retention laws limited individuals' ability to remain anonymous. He concluded that States should refrain from making the identification of users a condition for access to digital communications and online /services and requiring SIM card registration for mobile users.[36] This echoed the earlier recommendations, from 2013, on States to refrain from imposing such requirements as a pre-condition to use cybercafés or mobile telephony.[37]

- The Special Rapporteurs have also stressed that the disclosure of communication logs or data should be monitored by an independent authority such as a court. [38]

- From a comparative perspective, at European level, the Court of Justice of the European Union ('CJEU') has invalidated the Data Retention Directive, which imposed broad data retention requirements for a period between six months and two years. In particular, the Court considered that the Directive covered "in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime." Several constitutional courts across Europe have struck down data retention laws as incompatible with the right to privacy.

In ARTICLE 19's view, the requirements imposed by clause 7 are a wholly unjustified restriction of the rights to freedom of expression and privacy. In particular, Clause 7 does not expressly state what legitimate aim is sought to be achieved as a result of these various privacy-intrusive measures. To the extent that clause 7 implies that this is for the prevention of crime, these measures cannot be said to be necessary or proportionate for that purpose.

[36] See A/HRC/ 29/32 at para. 60.
[37] See A/HRC/23/40 at para. 88.
[38] *Ibid*. at 85-86.

We further consider that it is wholly unrealistic to expect cybercafés and public wireless hotspot providers to report cybercrime 'incidents' within 24 hours in the absence of a definition of either 'incident' or 'cybercrime'. In any event, we believe that cybercafés and public wireless hotspot providers should not be required to report such crimes as this presupposes that they should be monitoring their users communications or else lose their license. In our view, this would be both in breach of these operators' right to freedom of expression and the rights to freedom of expression and privacy of their users.

Recommendation:

- Clause 7 should be deleted in its entirety.

Data localisation requirements

Clause 10(1) requires the hosting and storage of public information within Kenya's boundaries. ARTICLE 19 notes, however, that the Cybersecurity Regulations fails to define 'public information'. It is unclear whether this covers information held by public authorities or information available on the Internet. In principle, this could include personal data of a wide range of individuals.

ARTICLE 19 further notes that other countries, such as Russia or Brazil, have attempted to adopt provisions requiring hosting providers to store data in their own countries. In ARTICLE 19's view, however, these measures tend to undermine the free flow of information and can be particularly problematic in countries without strong data protection laws. Moreover, they tend to be both costly for Internet intermediaries and impractical from a technical standpoint, as well as more likely to lead to loss of data than if it were stored in multiple locations globally.

Recommendation:

- Clause 10(1) should be deleted.

Electronic transactions regulations

Lack of basis for requiring service providers to be authorised

Clause 4 provides that service providers must obtain an authorisation from the Authority. Clause 2 defined 'service provider' as any person in Kenya who offers on a commercial basis, the sale, hire or exchange of goods or services through an electronic transaction.

ARTICLE 19 notes that the effect of Clause 4 is to impose the equivalent of a licensing requirement for the provision of goods and services online in Kenya. This is a wholly disproportionate restriction on freedom of expression. It is also clearly inconsistent with international standards on freedom of expression, which provide that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[39]

We further note that 'service providers' are not defined anywhere in the authorising statute, KICA, which primarily deals with providers of telecommunications and broadcasting services. As such, there are serious doubts that KICA provides any kind of legal basis for the Electronic Transactions Regulations.

Recommendation:

- Service providers should not be subject to an authorisation process, as such Clause 4 should be removed

Intermediary liability

Clauses 11 to 14 provide for the liability regime of service providers:

- Clauses 11 provides for relatively broad immunity from liability third party material (Clause 11 (1)) subject to certain exceptions, including the obligation of a network service provider under a licensing or other regulatory framework or a court order (Clause 11 (2)).
- Clause 12 provides for a separate liability regime for information location tools. Under clause 12, information location tools are granted immunity if the service provider: (a) does not have actual knowledge that the data message or activity is infringing the rights of the users; (b) is not aware of the facts or circumstances from which the infringing nature of the activity is apparent; (c) does not receive financial benefit directly attributable to the infringing activity, or (d) removes or disables access to the data message within a reasonable time after being informed that the data message or activity infringes the rights of the user.
- Clause 13 lays down the requirements of a valid notice of infringing data message or activity.
- Clause 14 (1) exempts service providers from an obligation to monitor the data, which they transmit, or store. They are also not required actively to seek facts or circumstances indicating unlawful activity. Clause 14 (2), however, provides that the Authority prescribe by way of statutory instruments the procedure for service providers to, among other things, inform the competent public authorities of any alleged illegal activities undertaken or information provided by recipients of their service;

In ARTICLE 19's view, while some of the above provisions are relatively positive such as clause 11 (1) or clause 14 (1), they are usually undermined by exceptions in sub-clauses and caveats elsewhere in the Regulations. For instance, under clause 11 (2), the broad immunity from liability does not apply to network service providers, who remain subject to licensing obligations. Similarly,

[39] See Joint Declaration on Freedom of Expression and the Internet, June 2011, *op.cit.*

under clause 14 (2) (a), the Authority retains broad powers to prescribe by way of statutory instruments the procedure for service providers to inform the competent public authorities of any alleged illegal activities undertaken or information provided by recipients of their service. Such statutory instruments could easily undermine the otherwise positive absence of monitoring obligations under Clause 14 (1). Moreover, Clause 15 gives broad powers to the authority to make guidelines by way of statutory instrument for any matter requiring it do so for the purposes of giving effect to the regulations. It could therefore easily undo some of the positive features outlined above.

ARTICLE 19 further notes that it is unclear why information location providers do not benefit from the more generous immunity from liability regime than other service providers. Instead, they are subject to a separate conditional immunity liability regime (clause 12), whose shortcomings are well-known (see international standards on freedom of expression section above). In our view, this distinction is hard to justify as a matter of principle.

Furthermore, we note that the threshold for material to be removed is too vague. In particular, the material only needs to be 'infringing' rather than 'unlawful'.[40] Since clause 12 seems to apply different thresholds of knowledge from 'actual knowledge' to 'awareness', it is unclear whether liability can be incurred for failure to remove access to content upon receipt of a valid notice or if a court order is required.

Recommendations:

- Clause 12 should be removed. Information location service providers should benefit from the same immunity from liability as other service providers.
- At a minimum, clause 12 should be amended as follows: (1) 'infringing' should be replaced with "unlawful"; clause 12 (b) to (d) should be removed; clause 12 (a) should specify that actual knowledge can only be obtained by a court order;
- Clauses 13 and 14 (2) (a) should be removed.
- Clause 15 should be removed as overly broad.
- KICA should be amended so that network service providers are no longer required to obtain a licence. This would make Clause 11 (2) (b) redundant.

Disclosure of user data

Clause 14 (2) (b) provides that the Authority may make guidelines for the procedure for service providers to communicate information enabling the identification of a recipient of the service at the request of a competent authority. In ARTICLE 19's view, this clause falls well below international standards on freedom of expression and privacy. In particular, user data should only be disclosed following a court order or an order of an independent adjudicatory authority. Moreover, it is entirely inappropriate that the Regulations are not laying down a clear procedure for the disclosure of user data. In the absence of such procedure, it is open to any authority to request access to user data without any meaningful procedural safeguards being put in place. Finally, it is inconsistent with the recommendations of the UN Special Rapporteur on Freedom of Expression.[41]

Recommendation:

- Clause 14 (2) (b) should be removed. User data should only be disclosed by a court order. Provision for such disclosure should be laid down in statute rather than regulations. At a minimum, it should be set out in detail in legal instruments rather than guidelines.

[40] We also note that clause 13 refers to information location tools referring users to 'intriguing' data messages. We assume that this is an error and that the regulations intended to refer to 'infringing' data messages.
[41] See A/HRC/ 29/32 at para. 60 and A/HRC/23/40 at para. 88.

Sanctions

Clause 16 provides that failure to comply with the Electronic Transations Regulations is an offence. However, clause 16 (1) does not provide for any specific punishment for such failure. Meanwhile, clause Article 16 (2) provides that in the absence of any express penalty, failure to comply with the regulations is an offence punishable by a term of imprisonment not exceeding 5 years or a fine not exceeding 1 million shillings.

In ARTICLE 19's view, this is both insufficiently clear and disproportionate in breach of international standards on freedom of expression. In practice, this means that failure to transmit all the notices of alleged illegality or failure to disclose the personal information of alleged infringers could be punished by potentially 5 years imprisonment or a 1 million fine. Similar sanctions could be applied to information location tools failing to remove links on notice.

Moreover, we note that the penalties imposed under Clause 16 (2) exceed the penalties prescribed by section 27 of KICA to which the Electronic Transactions Regulations appear to give affect. As such, they are *ultra vires* the authorising statute.

Recommendation:

- Failure to comply with the regulations should not be meted out with criminal penalties, let alone imprisonment. At a minimum, Clause 16 should be re-drafted to align with the relevant section of KICA.