

# Tanzania: Electronic and Postal Communications (Online Content) Regulations 2018

---

April 2018

# Executive summary

---

In this analysis, ARTICLE 19 reviews the compatibility of the Tanzania Electronic and Postal Communications (Online Content) Regulations 2018 (the Regulations) in the light of international standards on freedom of expression.

The Regulations were adopted on 16 March 2018 and issued pursuant to Section 103(1) of the Electronic and Postal Communications Act 2010, which grants powers to the Minister responsible for communications to make regulations upon recommendation of the Committee on content related matters.

Our analysis shows that the Regulations prohibit content in overly broad terms and impose confusing registration or licensing requirements which are in breach of international standards on freedom of expression. The lack of any clear definitions in the Regulations is especially concerning given that failure to comply with the regulations is punished with heavy sanctions, which include a minimum term of 12 months imprisonment, or minimum fines of five million Tanzanian Shillings, or both.

The Regulations also grant sweeping powers of content removal to the Tanzania Communications Regulatory Authority (TCRA), Tanzania's communications regulator. These powers contain no safeguards against abuse, and will almost certainly have the effect of stifling legitimate freedom of expression in Tanzania. These powers are therefore plainly incompatible with international human rights law.

**ARTICLE 19 concludes that the Regulations are so flawed that they should be withdrawn entirely.** Any proposal to regulate online content should be the subject of primary legislation, and should involve further discussion with all relevant stakeholders. We therefore suggest that the Regulations should be withdrawn in their entirety.

# Table of contents

---

<b>Introduction.....</b>	<b>4</b>
<b>International human rights standards .....</b>	<b>5</b>
The right to freedom of expression.....	5
Freedom of expression online and intermediary liability under international law .....	6
Online content regulation under international law .....	7
The protection of the right to privacy and anonymity online.....	7
<b>Analysis of the Regulations .....</b>	<b>9</b>
Vague and overbroad definitions.....	9
Powers of the Authority .....	11
The obligations of an online content providers .....	12
Obligations of subscribers, users and social media users .....	14
Obligations of application service licensees.....	14
Obligations of online radio, online television and bloggers.....	15
Obligations of online content hosts.....	15
Obligations of Internet cafes .....	16
Disclosure of information.....	16
Prohibited content .....	17
Complaints handling .....	19
Other provisions .....	20
Sanctions .....	20
<b>About ARTICLE 19.....</b>	<b>21</b>

# Introduction

---

In this analysis, ARTICLE 19 reviews Tanzania's Electronic and Postal Communications (Online Content) Regulations 2018 (the Regulations), published on 16 March 2018 by the Minister of Information, Culture, Arts and Sports. The Minister relies on Section 103(1) of the Electronic and Postal Communications Act 2010 as the legal basis for his power to issue the Regulations.

ARTICLE 19 notes that the Regulations seek to regulate the conduct of private companies and individuals in relation to the publication of and access to online content. It prohibits a wide range of content and creates new obligations and offences which constitute a serious interference with the rights to freedom of expression and privacy.

ARTICLE 19 considers that the obligations and offences created by the Regulations are so wide-ranging that it is deeply inappropriate to use subsidiary legislation (such as these regulations) rather than statute to create them. Among other things, the Regulations seek to prohibit 'hate speech', 'indecent', 'obscene' or 'false' content' – these prohibitions are framed in such overbroad language that would inevitably lead to the removal of legitimate expression.

The procedure for removal of content is entirely geared towards quasi-immediate removal of content (within 12 hours) by private companies on the say-so of individuals or a broad range of law enforcement agencies. Complaints are handled by the Tanzania Communications Authority, i.e. a public body, rather than the courts - there is no provision for a right of appeal or judicial review of content removal decisions.

The Regulations also impose confusing licensing requirements on undefined 'online service providers', as well as registration requirements on bloggers – all of this is in breach of international standards on freedom of expression.

ARTICLE 19 concludes that the 2018 Regulations are so flawed that they should be entirely withdrawn.

Our analysis is divided into two parts: first, ARTICLE 19 sets out international standards on freedom of expression; second, we analyse each part of the Regulations in turn.

# International human rights standards

---

ARTICLE 19's comments on the Regulations are informed by international human rights law and standards. The Regulations should also comply with the guarantees of freedom of expression in the Tanzania Constitution.<sup>1</sup>

## The right to freedom of expression

The right to freedom of expression is protected by Article 19 of the **Universal Declaration of Human Rights** (UDHR),<sup>2</sup> and given legal force through Article 19 of the **International Covenant on Civil and Political Rights** (ICCPR).<sup>3</sup> At the regional level, Article 9 of the **African Charter on Human and Peoples' Rights** (ACHPR)<sup>4</sup> guarantees the right to freedom of expression.<sup>5</sup> Tanzania ratified the ACHPR in 1984. Article II of the **Declaration of Principles on Freedom of Expression in Africa 2002** (African Declaration) further elaborates the protections to be afforded to the right to freedom of expression by States.<sup>6</sup>

The scope of the right to freedom of expression is broad. It requires States to guarantee to all people the freedom to seek, receive or impart information or ideas of any kind, regardless of frontiers, through any media of a person's choice. The UN Human Rights Committee (HR Committee), the treaty body of independent experts monitoring States' compliance with the ICCPR, has affirmed that the scope of the right extends to the expression of opinions and ideas that others may find deeply offensive.<sup>7</sup>

While the right to freedom of expression is fundamental, it is not absolute. A State may, exceptionally, limit the right under Article 19(3) of the ICCPR, provided that the limitation is:

- **Provided for by law**; any law or regulation must be formulated with sufficient precision to enable individuals to regulate their conduct accordingly.
- **In pursuit of a legitimate aim**, listed exhaustively as: respect of the rights or reputations of others; or the protection of national security or of public order (*ordre public*), or of public health or morals;
- **Necessary and proportionate in a democratic society**, i.e. if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the less restrictive measure must be applied.<sup>8</sup>

---

<sup>1</sup> The Constitution of the United Republic of Tanzania 1977, as amended (14th amendment of the Constitution, vide Act of Parliament No 1 of 2005, Article 18.

<sup>2</sup> Through its adoption in a resolution of the UN General Assembly, the UDHR is not strictly binding on states. However, many of its provisions are regarded as having acquired legal force as customary international law since its adoption in 1948; see *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2<sup>nd</sup> circuit).

<sup>3</sup> UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171. Tanzania ratified the ICCPR in 1976.

<sup>4</sup> 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).

<sup>5</sup> Article 9 of the ACHPR provides: (1) Every individual shall have the right to receive information; (2) Every individual shall have the right to express and disseminate his opinions within the law.

<sup>6</sup> Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights, 32nd Session, 17 - 23 October, 2002: Banjul, The Gambia.

<sup>7</sup> See HR Committee, General Comment No. 34 on Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, 12 September 2011, para 11.

<sup>8</sup> HR Committee, *Belichkin v. Belarus*, Communication No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

Thus, any limitation imposed by the State on the right to freedom of expression must conform to the strict requirements of this three-part test. Further, Article 20(2) ICCPR provides that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited by law (see below).

As a State party to the ICCPR, Tanzania must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 of ICCPR, as interpreted by the HR Committee, and that they are in line with the special mandates' recommendations. Tanzania should also take into account the principles developed in the African Declaration on Internet Rights, an initiative from African civil society organisations, which largely reflects the principles outlined in this section of our analysis.<sup>9</sup>

## Freedom of expression online and intermediary liability under international law

In 2012, the UN Human Rights Council (HRC) recognised that the “same rights that people have offline must also be protected online.”<sup>10</sup> The Human Rights Committee has also made clear that limitations on electronic forms of communication, or expression disseminated over the Internet, must be justified according to the same criteria as non-electronic or “offline” communications, as set out above.<sup>11</sup>

While international human rights law puts obligations on States to protect, promote and respect human rights, it is widely recognised that business enterprises also have a responsibility to respect human rights.<sup>12</sup> Importantly, the UN Special Rapporteur on freedom of opinion and expression (Special Rapporteur on FOE) has long held that censorship obligations should never be delegated to private entities.<sup>13</sup>

In his June 2016 report to the HRC,<sup>14</sup> the Special Rapporteur on FOE stipulated that States should not to require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extra-legal means. He further recognised that “private intermediaries are typically ill-equipped to make determinations of content illegality,”<sup>15</sup> and reiterated criticism of notice and takedown frameworks for “incentivising questionable claims and for failing to provide adequate protection for the intermediaries that seek to apply fair and human rights-sensitive standards to content regulation,” i.e. underlining the danger of “self- or over-removal” in these situations.<sup>16</sup>

The Special Rapporteur on FOE recommended that any demands, requests and other measures to take down digital content must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under Article 19 (3) of the ICCPR.<sup>17</sup>

Additionally, in their 2017 Joint Declaration, the four international mandates on freedom of expression expressed concern at “attempts by some governments to suppress dissent and to control

<sup>9</sup> The African Declaration on Internet Rights and Freedoms, available at <http://africaninternetrights.org/articles>.

<sup>10</sup> HRC Resolution 20/8 on the Internet and Human Rights, A/HRC/RES/20/8, June 2012.

<sup>11</sup> General Comment No. 34, *op cit.*, para 43.

<sup>12</sup> Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework (The Ruggie Principles), A/HRC/17/31, 21 March 2011, Annex. The HRC endorsed the guiding principles in the resolution 17/4, A/HRC/RES/17/14, 16 June 2011.

<sup>13</sup> Report of the Special Rapporteur on FOE 16 May 2011, A/HRC/17/27, paras. 75-76.

<sup>14</sup> Report of the Special Rapporteur on FOE, 11 May 2016, A/HRC/32/38; para 40 – 44,

<sup>15</sup> *Ibid.*

<sup>16</sup> *Ibid.*, para. 43.

<sup>17</sup> *Ibid.*

public communications through [...] efforts to 'privatise' control measures by pressuring intermediaries to take action to restrict content."<sup>18</sup> The Joint Declaration emphasises that:

[I]ntermediaries should never be liable for any third party content relating to those services unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that.

The four mandates also outlined the responsibilities of intermediaries regarding the transparency of, and need for, due process in their content-removal processes.

## Online content regulation under international law

The above principles have been endorsed and further explained by the Special Rapporteur on FOE in two reports, dated 16 May 2011<sup>19</sup> and 10 August 2011.<sup>20</sup> In the latter, the Special Rapporteur also clarified the scope of legitimate restrictions on different types of expression online.<sup>21</sup> He identified three different types of expression for the purposes of online regulation:

- 1) Expression that constitutes an offence under international law and can be prosecuted criminally. 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 criminalising 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;<sup>22</sup>
- 2) Expression that is not criminally punishable but may justify a restriction and a civil suit; and
- 3) Expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility, and respect for others.<sup>23</sup>

The Special Rapporteur on FOE 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 expression such as that "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 tranquillity."

## The protection of the right to privacy and anonymity online

The right to private communications is protected in international law through Article 17 of the ICCPR. 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.

<sup>18</sup> [Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda](#), adopted by the UN Special Rapporteur on FOE, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, 3 March 2017.

<sup>19</sup> Report of the Special Rapporteur on FOE, A/HRC/17/27, 16 May 2011.

<sup>20</sup> Report of the Special Rapporteur on FOE, A/66/290, 10 August 2011, para. 16.

<sup>21</sup> *Ibid.*, para. 18.

<sup>22</sup> *Ibid.*, para. 22.

<sup>23</sup> *Ibid.*

The UN Special Rapporteur on promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that, as with 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.<sup>24</sup> In 2017, the HRC confirmed this in Resolution 34/7.

Inability of individuals to communicate privately substantially affects their right to freedom of expression. In his report of 16 May 2011, the Special Rapporteur on FOE 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 individual's communications and activities on the Internet. Such practices can constitute a violation of the Internet user's 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 ensure that individuals can express themselves anonymously online, and that States refrain from adopting real-name registration systems.<sup>25</sup>

In May 2015, the Special Rapporteur on FOE published his annual report on encryption and anonymity in the digital age, in which he concluded:

Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective. (...)

60. States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. In addition, 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.<sup>26</sup>

The findings of this report confirmed the findings of the 2013 report of the Special Rapporteur on FOE, which observed that restrictions to anonymity facilitates States' communications surveillance and have a chilling effect on the free expression of information and ideas.<sup>27</sup>

<sup>24</sup> 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.

<sup>25</sup> *Ibid.*, para 84.

<sup>26</sup> Report of the Special Rapporteur on FOE, A/HRC/29/32, 22 May 2015, para 56.

<sup>27</sup> *Ibid.*, paras 48-49.

# Analysis of the Regulations

---

This analysis takes each of the Regulations' five parts in turn:

- Part 1 contains preliminary provisions, including definitions;
- Part 2 sets out the powers of the Tanzania Communications Regulatory Authority in relation to online content regulation;
- Part 3 lays out the obligations of online services providers;
- Part 4 concerns the handling of complaints; and
- Part 5 provides for offences and penalties for violations of the regulations.

We conclude that the Regulations are deeply flawed and entirely at odds with international standards on freedom of expression.

## Vague and overbroad definitions

ARTICLE 19 notes that the Tanzanian government has attempted to give a legal definition to several terms which are commonly used when referring to online activities. In particular, Part 1 of the Regulations sets out the definition of terms such as 'application services licensees', 'blogs', 'blogger,' 'content,' 'hate material', 'hate speech,' 'indecent material,' 'internet café,' 'law enforcement agency,' 'obscene content,' 'online forum,' 'online television,' 'prohibited content,' 'social media' and 'user.'

ARTICLE 19 is concerned that the vast majority of these definitions are overly broad and fail to meet the legality requirement of international human rights, particularly in light of the sweeping powers granted to the Tanzania Communications Regulatory Authority (see next part of this analysis):

- **"Hate material"** is defined as "content, which advocates or promotes genocide or hatred against an identifiable group of people." The scope of this definition is overbroad. To begin with, it conflates different types of expression. "Hate material" is likely to be confused with 'hate speech,' a term which is itself ill-defined (see below). It appears that the drafters intended the definition of "hate material" to include references to both "direct and public incitement to commit genocide" and a much broader version of the prohibition of "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence" under Article 20(2) of the ICCPR. However, none of the terms used in the definition comply with the requirements of international law.

ARTICLE 19 notes that under international law, "incitement to commit genocide" must be both "direct" and "public." These important qualifiers are missing from the definition. Moreover, given that incitement to commit genocide is prohibited by international criminal law, a vague reference in secondary legislation is clearly inadequate to comply with the relevant international law requirements. At the very least, such offence should be clearly laid down in Tanzania's criminal code, and the Regulations should then make reference to that provision.

The reference to "advocacy of hatred against an identifiable group of people" entirely ignores the wording of Article 20(2) of the ICCPR, which prohibits the advocacy of *national, racial or religious* hatred that constitutes *incitement to discrimination, hostility or violence*." Again, the definition of "hate material" merely refers to feelings of intense and irrational emotions of opprobrium, enmity and detestation towards groups which are not defined by reference to any protected characteristics under international law.<sup>28</sup> As such, any power to block or remove access to "hate material" is likely to be applied to vast amounts of legitimate expression.

---

<sup>28</sup> The [Camden Principles on Freedom of Expression and Equality](#), ARTICLE 19 (2009), Principle 12.1.

- **“Hate speech”** is defined in the Regulations as ‘any portrayal by words, speech or pictures or otherwise, which denigrates, defames, or otherwise devalues a person or group on the basis of race, ethnicity, religion, nationality, gender, sexual orientation, or disability.’ ARTICLE 19 notes that there is no agreement on the meaning of the term ‘hate speech’ under international law. By contrast, Article 20(2) of the ICCPR prohibits the advocacy of “national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence” – this is thus the terminology which ought to be used in primary or secondary legislation.

In ARTICLE 19’s view, the definition of ‘hate speech’ in the Regulations is inadequate and inconsistent with international standards on freedom of expression. In particular, we note that the definition again conflates various concepts, including “incitement to discrimination, hostility or violence” and “defamation” “denigration” or “devaluation.” The Camden Principles on Freedom of Expression and Equality define the terms ‘hatred’ and ‘hostility’ as the “intense and irrational emotions of opprobrium, enmity and detestation towards the target group.”<sup>29</sup>

By contrast, defamation law seeks to protect the reputation of individuals against false statements of fact, which tend to lower the esteem in which they are held in their community.<sup>30</sup> Its purpose is different from “hate speech” law. Similarly, the terms “denigrating” or “devaluing” are highly subjective and liable to be interpreted in such a way that it includes content that is deemed offensive by particular groups. These terms are therefore broader than ‘incitement’ to discrimination. Thus, the definition of “hate speech” in the Regulations is overbroad and likely to restrict legitimate expression.

- **“Indecent material”** is broadly defined as “any content which is offensive, morally improper and against current standards of accepted behaviour such as nudity and sex.” This definition provides no clarity or guidance whatsoever as to what is meant by indecent material. Instead, it introduces other vague and subjective terms, such as ‘offensive’, ‘morally improper’, and ‘against current standards of accepted behaviour’, which are clearly open to a variety of interpretations. ARTICLE 19 notes that pornography is a legitimate form of expression under international human rights law, though some restrictions on access to that material may be permitted. Given the already-sweeping censorship powers of the Tanzania Communications Regulatory Authority, legitimate content would inevitably be removed under this definition (e.g. a painting depicting a nudity, such as *L’Origine du Monde* by Gustave Courbet).<sup>31</sup>
- **“Obscene content”** is defined as content which “gives rise to a feeling of disgust by reason of its lewd portrayal and is essentially offensive to one’s prevailing notion of decency and modesty with a possibility of having a negative influence and corrupting the mind of those easily influenced.” In ARTICLE 19’s view, this definition is excessively vague and would inevitably reflect the subjective notions of decency held by members of the Tanzania Telecommunications Regulatory Authority. In any event, the definition does not explain what “prevailing notions of decency and modesty” entail or how that conclusion would even be reached/on what basis that analysis would be made. It also displays a patronising attitude towards the public, and implies that the public is seemingly deemed incapable of forming its own judgment on the basis of available information.
- **‘Application services licensee,’ ‘blogs,’ ‘bloggers,’ ‘users,’ and ‘online television’** are terms which are defined either too broadly or too narrowly, and often overlap. For instance, ‘application services licensee’ is defined as a “licensee of the Authority in the category of application service licence limited to the provision of online content or the facilitation of online content producers.” It is unclear, however, who is a provider of ‘online content’ or what is deemed to ‘facilitate online content producers.’ The definition could cover ‘bloggers’, ‘social

<sup>29</sup> *Ibid.*

<sup>30</sup> ARTICLE 19, [Defining Defamation: Principles on Freedom of Expression and the Protection of Reputation](#), 2017.

<sup>31</sup> C.f. Facebook Finally Lands In French Court For Deleting Nude Courbet Painting, Forbes, 5 February 2018.

media companies', or individuals creating webpages or online forums which enable interaction between Internet users.

By contrast, the definition of "users" is relatively narrow: it is limited to a person or legal entity "accessing online content, whether by subscription or otherwise." In practice, users of online services rarely limit themselves merely to *accessing* online content. They use the various tools available on social media and other platforms to *engage* with the content and post comments, share news articles etc. In this sense, users are also producers of content. The Regulations themselves recognise this (see Regulation 5(2)).

Meanwhile, the definitions do not clearly articulate the difference between 'users' and 'bloggers' who are defined as "writers or groups of writers owning or performing the act of blogging and any other acts similar to bloggers." Notwithstanding the lack of definition of blogging, 'blogs' cover the sharing of "experiences, observations, opinions including on current news, events" and video clips and links to other websites. In other words, this includes the sort of activity that most Internet users are engaged in on the Internet.

Other examples of overbroad definitions include "online television," which encompasses the distribution of videos created by individuals. In other words, 'users' and 'bloggers' are equated with 'online television' for the purposes of the Regulations.

- **"Law enforcement agency"** includes the intelligence services (despite the fact that they perform different functions) and "any authority responsible for regulating communications or in any other body authorised in any written law." In other words, the Regulations implicitly grant any government agency the same powers as traditional law enforcement agencies, e.g. to require cooperation from content providers or content service providers. This is both plainly overbroad, but it is also outside the competence of the Minister Information, Culture, Arts and Sports to grant such powers (see next section).
- Finally, certain key terms, which are repeatedly used throughout the Regulations, are not defined at all, e.g. 'online content provider' in Regulations 5 and 12. This is particularly problematic, as it is material to whether providers need to obtain a licence.

## Powers of the Authority

Part 2, Regulation 4 of the Regulations sets out the powers of the Communications Regulatory Authority. These include: (i) the keeping of a register of bloggers, online forums, online radios and televisions; and (ii) action against non-compliance with the Regulations, including ordering the removal of 'prohibited content.'

The government argues that the legal basis for these powers is contained in Section 103(1) of the Electronic and Postal Communications Act 2010, which grants powers to the Minister responsible for communications to create regulations, upon recommendation of the Committee on content related matters.

ARTICLE 19 note, however, that the powers laid down in Regulation 4 seriously interfere with the fundamental rights to freedom of expression and privacy. As such, we consider that Section 103(1) of the Electronic and Postal Communications Act 2010 is an insufficient legal basis for the creation of the 2018 Regulations. Such intrusive powers, should be laid down in primary legislation, if at all. In any event, both the registration of bloggers etc. and the power to order the removal of prohibited content are incompatible with international standards on freedom of expression.

We have the following comments on the powers of the Communications Regulatory Authority:

- **Registration of bloggers, online forums, online radios and televisions:** ARTICLE 19 notes that the power to register online forums, online radio and online televisions is incompatible with international standards on freedom of expression. In particular, the 2011 Joint Declaration on Freedom of Expression and the Internet provides that measures such as imposing registration and other requirements on service providers is not legitimate, unless such measures conform to the three-part test on lawful restrictions of freedom of expression under international law.<sup>32</sup> At most, a requirement to declare a business, rather than a requirement of registration, may be imposed. As regards the registration of bloggers, the Human Rights Committee has made it clear (in General Comment no. 34) that ‘journalism’ is a *function* shared by many different actors, including bloggers. The Committee has also reiterated that mandatory registration of journalists is a disproportionate restriction on freedom of expression. Accordingly, the mandatory registration or licensing of bloggers or any member of the general public engaged in journalistic activity is incompatible with the right to freedom of expression.<sup>33</sup> In any event, it has no plausible justification.<sup>34</sup>
- **Powers to order the removal of prohibited content:** Under international law, powers to order the removal of content should rest with the courts.<sup>35</sup> At a minimum, removal orders should be made by independent authorities, and should be subject to judicial review. This is plainly not the case here: the Tanzania Communications Regulatory Authority (the Authority) is not independent and the Regulations do not provide for a right of appeal, or judicial review of takedown orders. Moreover, it is unclear whether the Authority can exercise its power to order content takedown of its own initiative, or only upon notification of non-compliance (Part 4, Handling Complaints).

## The obligations of an online content providers

Part 3 of the Regulations contains the obligations of various actors involved in online content. Regulation 5(1) sets out the obligations for “online content providers and users.” ARTICLE 19 notes that a key term, ‘online content provider’, has not been defined. It is not clear if ‘online content provider’ refers to social media platforms, hosts, and other third party entities, or if the term refers to authors or publishers of various types of content online such as newspapers.

If “online content providers” refers to authors or publishers of various types of content online, including newspapers and others, then most of the obligations set out in Regulation 5(1) are redundant and unnecessary, given that they already correspond to the rules and practices followed by publishers. Moreover, it is worth remembering that everyone is required to comply with the law.

Insofar as media, bloggers, and users may also be acting as hosts for the purposes of third-party content, e.g. by allowing posts by third parties in the ‘Comments’ section of their website, the obligations set out in Regulation 5(1) are problematic and inconsistent with international standards on freedom of expression and privacy. The same is true insofar as ‘online providers’ encompasses social media platforms and similar services.

- Regulation 5(1) (a) requires online content providers to ensure that their online content is “safe, secure and does not contravene the provisions of any written law.” In ARTICLE 19’s view, it is highly unclear what the expression “safe and secure” means. For instance, it could be understood to mean the adoption of policies on online content such as harassment, or it could mean the adoption of policies and tools enabling anonymity. There is no way of knowing, as the Regulations do not provide any further definitions. The expression ‘any written law’ is also ambiguous. Although everyone, whether individuals or legal persons, is required to comply with

<sup>32</sup> 2011 Joint Declaration, *op.cit.*, para 6(d).

<sup>33</sup> ARTICLE 19, [The Right to Blog](#), 2013, p. 16.

<sup>34</sup> *Ibid.*

<sup>35</sup> ARTICLE 19, [Internet Intermediaries: Dilemma of Liability](#), 2013, p. 17.

the law, the latter expression could be interpreted as a form of strict liability for third-party content. This is especially important given that failure to comply with the Regulations is a punishable offence (see last section). In other words, Regulation 5(1) falls well below the legality requirement under international law. Moreover, it is likely to lead to greater censorship of legitimate content, and therefore constitutes a disproportionate restriction on freedom of expression.

- Regulation 5(1)(b) requires content providers to take trends and cultural sensitivities of the general public into account. This obligation is both overbroad and unnecessary and would be an entirely subjective analysis. It is highly unclear what this obligation entails, in the absence of more detail about what trends are being referred to (political, economic, social etc.) and what 'cultural sensitivities' are. In practice, this obligation could either be very onerous, or discharged with minimal effort. In any case, this requirement cannot be justified as necessary for the pursuit of any of the legitimate aims under Article 19 (3) of the ICCPR.
- Regulation 5(1)(d) requires online content providers to use moderating tools to filter prohibited content. In ARTICLE 19's view, hosts and other 'online content providers' should not be required to moderate content. To do so is to put them in the position of having to decide the legality of content, which is deeply inappropriate and in breach of international standards on freedom of expression. Moreover, obligations to monitor and filter content raise significant privacy concerns. For these reasons, the free speech mandates affirmed in their 2011 Joint Declaration that States should not impose general obligations to monitor content.<sup>36</sup> Principle 29 of The Global Principles on Protection of Freedom of Expression and Privacy – a broad civil society initiative - also states that intermediaries should not be required to monitor their services actively, to prevent privacy infringements.<sup>37</sup>
- Regulation 5(1)(e) requires content providers to have mechanisms in place in order to identify the source of content. ARTICLE 19 is concerned by the impact this obligation will have on citizens, journalists, and whistle-blowers who rely on secure and private communications to express themselves freely and carry out their duties. Even more alarming is the broad and unfettered power of surveillance that is being given to content providers. This obligation is in breach of both the rights to privacy and freedom of expression.<sup>38</sup> We further note that the Special Rapporteur on freedom of expression has recommended that the use of anonymity and encryption tools should be protected and promoted rather than unduly limited.<sup>39</sup>
- Regulation 5(1)(f) requires online content providers to "take corrective measures for objectionable or prohibited content." ARTICLE 19 notes that the Regulations introduces a new term 'objectionable content', which is not defined in the definitions section in Part I. It is also excessively broad: in practice, it means that online content providers could remove all kinds of speech, both legal and illegal, under domestic and international human rights law. It is also unclear whether online service providers would be required to do this of their own accord on the basis of the monitoring obligation outlined above, or upon notice or complaint. In any event, online content providers should be free to moderate content on their platforms in line with their own values and the type of environment they seek to promote (e.g. safe platform for children). They should not be required to do so, even less on the basis of such vague terms.
- Regulation 5(1)(g) requires online content providers to ensure that prohibited content is removed within 12 hours of being notified. Again, the Regulations are excessively vague on this point. In particular, they are silent on whether this notification must be given by a court, the regulatory authority, or simply by a user. In any event, as explained below, the entire proposed content-removal process of the Regulations fails to comply with international standards on

<sup>36</sup> The 2011 Joint Declaration, *op.cit.*

<sup>37</sup> ARTICLE 19, [the Global Principles on Protection of Freedom of Expression and Privacy](https://www.article19.org/resources/wp-content/uploads/2017/04/Global-Principles-on-Protection-of-Freedom-of-Expression-and-Privacy-2017.pdf), 2017.

<sup>38</sup> Report of the Special Rapporteur on FOE, A/HRC/23/40, 17 April 2013, para.79.

<sup>39</sup> *C.f.*, The May 2015 Report of the Special Rapporteur on FOE, *op.cit.*, para.63.

freedom of expression. It contains no due process safeguards (e.g. counter-notice, appeals etc.) and will inevitably result in the removal of legitimate expression.

- Regulation 5(3) requires online content providers to cooperate with law enforcement. No further indication is given as to how that cooperation might take place. It is entirely lacking in procedural safeguards for the protection of the rights to privacy and freedom of expression of users of the platform or online service. For instance, no reference is being made to the need for a judicial warrant in order to access users' personal information, nor is any reference made to the need for a judicial order insofar as cooperation may involve the removal of content. As such, this Regulation fails to comply with international standards on freedom of expression and privacy.

## Obligations of subscribers, users and social media users

Regulation 5(2) sets out the obligations of subscribers and users. Regulation 5(2)(a) provides that users and subscribers are accountable for the information they post online, while Regulation 5(2)(b) stresses that users must ensure that their posts do not contravene the Regulations or any other written law. Regulation 10 essentially repeats the same obligations in relation to social media users with an added requirement to create a password 'to protect user equipment.'

ARTICLE 19 considers that these Regulations are redundant as they merely re-state that everyone should comply with the law, or in the case of the obligation to create passwords, reflect best practice. It is also unclear how such an obligation would be enforced. In any event, we note that the Regulations themselves fail to meet the legality requirements in too many ways to provide any adequate guidance to users and others as to what is or is not permitted.

## Obligations of application service licensees

Regulation 6 sets out the obligations of application service licensees. As we have said, the definition of an application service licensee is ambiguous, and too vague. It is not clear whether it is applicable to application developers, social media platforms, Internet Service Providers, online TV, or other entities.

- **Delegating censorship powers by contract:** Regulation 6(1)(a) provides, *inter alia*, that application service licensees are required to include contractual terms which give the companies a right to "deny or terminate their service where a subscriber contravenes the Regulations." ARTICLE 19 notes that online service providers' Terms of Service frequently provide that their service should only be used in accordance with the law and that any breach of the Terms of Service or other company policies may lead to the suspension or termination of the service. However, the Regulations are seemingly designed to delegate content removal powers to online service providers and put them in the position of enforcers of the law. This is confirmed by Regulation 6(1)(b), which requires online service providers to include terms allowing them to "remove content in accordance with the Regulations." In our view, this is deeply inappropriate and inconsistent with international standards on freedom of expression and intermediary liability as outlined in Part I of this legal analysis.<sup>40</sup>
- **Content removal procedure:** Regulation 6(3) to (5) outlines the obligations of application service licensees in relation to content removal. Under Regulation 6(3), licensees are required to inform subscribers that they must remove content, and do so within 12 hours of receiving notice from the regulatory authority or a person affected by the prohibited content. Subscribers then have 12 hours to remove the content. If the subscriber fails to remove the content within

<sup>40</sup> See also [Manila Principles on Intermediary Liability](#).

12 hours, the licensee must suspend or terminate the subscriber's access to the service. This procedure plainly fails to include any due process safeguards. To begin with, notice that content must be removed should only ever be made by a court or independent adjudicatory body, and not by a regulatory authority or an individual. Only a court is able to determine the legality of content. Moreover, the procedure fails to include basic procedural safeguards, including the opportunity for individuals (those whose content is alleged to be unlawful) to challenge the allegation *before* content is taken down, as well as lacking a mechanism for the provision of reasons for the removal, and providing a right of appeal. The sanction for failing to remove content within 12 hours is also disproportionate given that subscribers are given an incredibly short period of time to comply or raise any objections. In other words: the procedure for the removal of content under the Regulations is fundamentally flawed.

## Obligations of online radio, online television and bloggers

Regulation 7 provides for the obligations of online radio, online television, and bloggers. Regulation 7(1) applies various traditional broadcasting requirements to online radio and television. While this is not problematic *per se*, the extension of those requirements to bloggers is worrying, as well as inconsistent with international standards on freedom of expression:

- **Licensing bloggers:** Regulation 7(2), read in conjunction with Regulation 7(1), means that bloggers are subject to the same requirements as online radio and television. It remains unclear however whether bloggers are required to obtain a licence with the Authority, or a simple registration is sufficient. In any case, as previously noted, mandatory registration or licensing of bloggers is inconsistent with international standards on freedom of expression: it serves no legitimate purpose and is unnecessary.<sup>41</sup>
- **Jurisdiction:** Regulation 7(2) extends the application of licensees' obligations to Tanzanian citizens residing outside the country, and blogging or running online forums with contents for consumption by Tanzanians. ARTICLE 19 is concerned by the extraterritorial application of these provisions. While the enforcement of the law can be a daunting task because of the cross-border nature of the Internet, this should not be used as an excuse for the adoption of overbroad extraterritorial provisions. This is especially the case when the substantive provisions of the law are incompatible with international standards on freedom of expression. In our view, domestic provisions should only apply extraterritorially when a real and substantial connection can be established between the service at issue and the country seeking to apply its laws in this way.<sup>42</sup> This would be the case, for instance, where the content is uploaded in Tanzania or where the content is specifically directed at Tanzania.
- **Licensing of electronic media:** Under Regulation 7(3), "electronic media" are required to apply for a licence. As noted above, any kind of licensing of journalists, bloggers, or electronic or print media is incompatible with international standards on freedom of expression. The information required to obtain a licence does not serve any legitimate aim and is plainly unnecessary.

## Obligations of online content hosts

Regulation 8 sets out the obligations of online content hosts. These include the adoption of a code of conduct for hosting content and the removal of content upon notification by persons affected by the content, the Authority or law enforcement. ARTICLE 19 reiterates that the removal of content should only take place after a court or other independent adjudicatory body has determined that the content complained of was unlawful. It is deeply inappropriate and inconsistent with international

---

<sup>41</sup> The Right to Blog, *op.cit.*, p.18.

<sup>42</sup> *Ibid.*, para 4(a).

standards on freedom of expression for content to be removed simply on the request of individuals. This will plainly lead to the removal of content that individuals find merely offensive, but that is not otherwise unlawful as such. Equally, the decision of a regulatory authority or law enforcement should not be considered sufficient to decide the legality of content. At a minimum, if an independent public authority takes such a decision, it should be subject to appeal or judicial review.

We reiterate that the procedure put in place under the Regulations for the removal of content by various actors fails to provide for adequate due process safeguards. It is in breach of international standards on freedom of expression.

## Obligations of Internet cafes

Regulation 9 provides for various obligations of Internet cafes, including a requirement to:

- filter prohibited content;
- install video cameras to record the activities of Internet users inside the cafe. The surveillance video recordings and information registered must be kept for a period of 12 months; and
- register all Internet cafe users upon showing of an ID card.

ARTICLE 19 notes that these requirements significantly interfere with the right to freedom of expression; they should therefore have a proper basis in law, i.e. statute, rather than in secondary legislation. Furthermore, the purpose of these measures remains unclear.

In any event, they are disproportionate to any of the legitimate aims under international human rights law. First, we note that prohibited content is so broadly defined in these Regulations that the mandatory application of filters will inevitably result in the filtering of legitimate content.

Secondly, the Special Rapporteur on FOE has made clear that the mandatory registration of Internet users was incompatible with international standards on freedom of expression.

Thirdly, the installation of surveillance cameras in commercial premises, i.e. private property, cannot be justified by reference to the protection public safety or any other legitimate aim. While it may be legitimate for businesses to install surveillance cameras in their premises to prevent e.g. shoplifting, this decision should be left to them, not imposed by the State.

## Disclosure of information

Regulation 11 lays down some safeguards for the protection of the right to privacy as regards the disclosure of personal information. In particular, Regulation 11(1) provides that personal information can only be disclosed upon request by a court, a lawfully constituted tribunal, or a law enforcement agency.

Under Regulation 11(2), the sharing of personal information with other public authorities can only take place if necessary for the performance of public duties.

Although these safeguards are welcome, in our view they are too limited. To begin with, the power to share personal data should be laid down by statute rather than secondary legislation. Secondly, the broad definition of 'law enforcement agency' means that a large number of public authorities can easily gain access to personal information held by private parties, simply upon request.

We believe that access to such data by public authorities should, in principle, require a judicial warrant with some permitted exceptions for law enforcement and intelligence agencies in limited circumstances.<sup>43</sup> Thirdly, any legislation concerning access or disclosure of personal data should

<sup>43</sup> See Necessary and Proportionate Principles: <https://en.necessaryandproportionate.org>.

make explicit reference to the protection of the right to privacy as a factor when considering whether disclosure is necessary and proportionate in the circumstances. Further, it should also make explicit reference to data protection legislation, if any; if such legislation does not exist, it should be adopted as a matter of urgency.

## Prohibited content

Regulation 12 lists various types of ‘prohibited content.’ ARTICLE 19 is concerned that the list prohibits content that may not be explicitly banned under Tanzanian law, or content that is legitimate under international human rights law.

In any event, the list of prohibited content contains several terms that are unduly vague. Legitimate content will inevitably be affected, and even removed, as a result. We highlight particular points of concern further below.

- **Hate speech, obscene and indecent content:** Regulation 12 (a), (b), and (c) prohibit indecent content, obscene content and hate speech. However, as we already noted, the definition of these terms in the Regulations is overly broad. It is also unclear how they might relate to the prohibition of equivalent content under domestic legislation and whether the latter is broader or narrower. This is likely to result in greater legal uncertainty.
- **Pornography:** Regulation 12(d) prohibits “explicit sex acts” and “pornography.” We note that the distinction between the two is unclear. At any rate, outright bans on pornography constitute a disproportionate restriction on freedom of expression. Access to pornography may, however, legitimately be restricted, for example through privacy-compliant age verification systems.
- **Sexual offences:** Regulation 12(e) bans the publication of sex crimes, rape, attempted rape, statutory rape, and bestiality. Although ARTICLE 19 understands the concerns of regulators that access to certain types of material should be restricted, particularly in the case of a younger audience, we consider that this provision is drafted in overly broad terms. Once again, the regulation is drafted as an outright ban rather than mere restriction on access. Furthermore, the regulation does not distinguish between works of fiction (e.g. cinematic films) and reality, nor does it provide for exceptions for legitimate reporting on these matters or educational material, e.g. sex education etc. It is also unclear whether the above only applies to video material or also includes written text.
- **Violent content:** Regulation 12(f) bans the publication of content that ‘portrays violence, whether physical, verbal or psychological, that can upset, alarm, and offend viewers, and cause undue fear among the audience or encourage imitation.’ ARTICLE 19 considers that this category of content is excessively broad. It is also eminently subjective and encompasses content that individuals may find merely offensive. It is also entirely unclear how anyone can predict what conduct is likely to ‘encourage imitation.’ ARTICLE 19 notes that rather than imposing outright bans, it would be more appropriate for the government to consult on the extent to which content rating systems should be applied to e.g. video-sharing platforms.<sup>44</sup> We note, for instance, that companies like YouTube already use interstitial warnings for certain types of violent videos.<sup>45</sup> If individuals do not want to be exposed to some categories of content, they should be offered the possibility of using filters for that purpose. However, the decision to use filters should be left to individuals rather than imposed by the State, for the reasons outlined above.

---

<sup>44</sup> See e.g. Age ratings enforced for UK-produced music videos on YouTube and Vevo, The Guardian, 18 August 2015.

<sup>45</sup> See e.g. YouTube will hide, but not remove, some ‘supremacist’ videos, The Verge, 1 August 2017.

- **Torture, killings etc.:** Regulation 12(g) prohibits content portraying sadistic practices and torture, explicit and excessive imagery of injury and aggression, and of blood or scenes of execution or of people clearly being killed. In ARTICLE 19's view, the ban on this type of content raises the same issues as those outlined in relation to Regulation 12(e) and 12(f). It fails to take into account public interest reporting on these matters or the nature of the video at issue, for instance whether it is a work of fiction, educational content etc. As such, perfectly legitimate content is likely to be removed in breach of international standards on freedom of expression.
- **Annoyance, threats of harm, public disorder:** Regulation 12(h) prohibits "content that causes annoyance, threatens harm or evil, encourages or incites crime, or leads to public disorder." This category is plainly overly broad. Whether content causes 'annoyance' is clearly a subjective matter and it should therefore not be prohibited. For example, politicians might find some legitimate public interest reporting 'annoying.' It would plainly be improper if such individuals could merely point to the Regulations and request the takedown of content on that basis. The definition of other terms remains mysterious. For instance, it is unclear what a threat of 'evil' entails. Given the breadth of what may be criminalised under Tanzanian law, the prohibition on 'encouraging or inciting crime' would almost inevitably include legitimate material. It is also unclear how it would be determined that content would lead to public disorder. For instance, the video of a young man setting himself on fire sparked the Tunisian Revolution in 2011. However, this was not foreseeable and, in any event, the availability of this video was a matter of public interest - it showed the desperate situation of some members of Tunisian society.

ARTICLE 19 recalls that under international law, only incitement to commit genocide, incitement to terrorism and incitement to discrimination, hostility or violence must be prohibited. Other restrictions on freedom of expression must meet the requirements of the three-part test of legality, necessary and proportionality. This is plainly not the case in regard to the vast majority of the terms in Regulation 12(h). While 'threats of harm' may be a more legitimate ground for content removal by a court, it should be further narrowed to threats of *serious* harm. In any event, it is important to remember that, insofar as someone makes a credible threat that they will commit e.g. assault, they should be investigated and prosecuted as appropriate. In such cases, a video message conveying the threat is a piece of evidence that should be preserved to that effect.

- **Hate propaganda, hatred etc.** Regulation 12(i) prohibits content 'which advocates hate propaganda, or promotes genocide or hatred against an identifiable group.' However, as noted above, this category of content is drafted in overly broad terms. It is also confusing and redundant given other categories of prohibited content such as Regulation 12(c).
- **National security, public health and safety:** Regulation 12(j) prohibits a raft of categories of content on national security and public health and safety grounds. This includes, *inter alia*, information about potential terrorist attacks, disturbances in parts of the country and outbreaks of deadly or contagious diseases, as well as false information about outbreaks of racial [hatred] and the publication of illegal bomb- or drug-making manuals and counterfeit products. ARTICLE 19 notes at the outset that it is legitimate for the authorities to seek to restrict broad public access to bomb-making manuals.

We also recognise that public authorities may legitimately seek to limit the release of information available to them for a period of time about e.g. terrorist attacks, outbreaks of deadly disease, particularly in fast-moving scenarios where intelligence operations might be under way and facts may be difficult to ascertain. However, Regulation 12(j) is drafted in much broader terms than this. As currently drafted, this provision prevents the legitimate reporting of matters which are clearly in the public interest (terrorist activity, disturbances in the country, health and safety concerns related to deadly disease etc.). It could be used to prosecute

journalists, researchers, environmental activists, human rights defenders, or others, for disseminating such information.<sup>46</sup>

- **Bad language:** Regulation 12(k) prohibits content that uses bad language, including (i) “the use of disparaging or abusive words which is calculated to offend an individual or a group of persons,” (ii) “crude references words in any language commonly used in the United Republic, which are considered obscene or profane including crude references to sexual intercourse and sexual organs;” and (iii) hate speech. In ARTICLE 19’s view, this provision is plainly inconsistent with international standards on freedom of expression. We recall that freedom of expression protects speech that offends, shocks, or disturbs: this Regulation would lead to the removal of legitimate content. It is only in circumstances where such language can be said to amount to advocacy of hatred that constitutes incitement to discrimination, hostility or violence that it can be prohibited.
- **False content:** Regulation 12(l) prohibits false content which is likely to mislead or deceive the public, save where it is clearly pre-stated that the content at issue is a parody, fiction, not factual. ARTICLE 19 notes that this provision, like the others, is drafted in excessively broad language. In particular, it fails to take into account the inherent difficulty in distinguishing fact from opinion. We are very concerned that it will be abused to crack down on opinions that the government does not like. The limited exceptions under Regulation 12(l) - (i) to (iii) - do nothing to alleviate concerns. They also impose undue burdens on individuals to determine and ‘pre-state’ whether information they are sharing is fact or fiction, which they may not be in a position to do. In our view, this provision is hopelessly flawed and incompatible with international standards on freedom of expression. In particular, the four mandates on freedom of expression recently reaffirmed that vague prohibitions on the dissemination of information such as “false news” are inconsistent with international standards for limiting freedom of expression.<sup>47</sup>

## Complaints handling

Part 4 (Regulations 16 and 17) of the Regulations lays down the procedure for handling complaints about prohibited content. If a person feels aggrieved by any matter related to prohibited online content, they may file complaints to the online content provider. On receipt of such complaint, the online content provider must ‘resolve’ the content being complained of within 12 hours. If the online content provider fails to remove the content, the aggrieved person may, within thirty days refer the complaint to the Authority. The Authority then serves a copy of the complaint to the online service provider, who must respond within 12 hours. If the complainant is still not satisfied with the response of the content provider, the matter is handled under the Content Committee Procedures of the Authority.

In ARTICLE 19’s view, the content removal procedure is deeply flawed and in breach of international standards on freedom of expression, as outlined in Part 1 of this analysis.<sup>48</sup> To begin with, the entire process is based on overbroad content prohibitions.

Secondly, the process is designed so that content is removed on the mere say-so of private parties or law enforcement agencies, or left to the discretion of the Authority, which is neither a court nor an independent body.

Thirdly, there is no opportunity for the publisher of the content to have their views heard before a decision is taken to remove the content. Additionally, 12 hours is clearly an insufficient period of time to review complaints properly.

<sup>46</sup> General Comment No.34, *op.cit.*

<sup>47</sup> The 2017, the Joint Declaration, *op.cit.*

<sup>48</sup> See also Manila Principles, *op.cit.*

Fourthly and lastly, there is no right of appeal or judicial review of the decisions taken by the Content Committee.

## Other provisions

Regulation 13 (protection of children), 14 (application for online content service licence) and 15 (cancellation of online content service licence) are, by comparison, less controversial. Nonetheless, ARTICLE 19 finds that they do fail to comply with the legality requirement under international law. For instance, Regulation 13 imposes obligations on online content service providers to ensure that children do not register, access or contribute to online prohibited content. While some restrictions on access to certain types of content by children may be justified, it is entirely unclear online content service providers are supposed to implement these obligations. This is problematic given the harsh sanctions for failure to comply with the Regulations (see below).

Similarly, the lack of clear definition of ‘online content service provider’ means that some actors may fail to obtain a licence when they should. In our view, broadcasting-type licences should only be required for broadcasting-like content rather than content produced by online newspapers, bloggers and Internet users). Finally, we note that the Regulations fail to provide for - or refer to any existing legislation providing for - an appeal procedure if a licence is cancelled by the Authority.

## Sanctions

Part 5 of the Regulations provides that failure to comply with the Regulations is an offence punishable with a minimum fine of five million Tanzanian shillings, or with imprisonment for a minimum period of twelve months or both.

ARTICLE 19 reiterates that the creation of new offences should not be left to statutory instruments but, if at all, should be adopted by primary legislation. We also note that these penalties are incredibly heavy and are highly likely to have a chilling effect on online freedom of expression in Tanzania.

## 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, freedom of expression and equality, 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 [www.article19.org](http://www.article19.org).

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](mailto:legal@article19.org).

For more information about the ARTICLE 19's work in East Africa, please contact Henry Maina, Director of ARTICLE 19's East Africa office at ARTICLE 19, at [henry@article19.org](mailto:henry@article19.org).