Rwanda: 2016 Law Governing Information and Communication Technologies

May 2018

Legal analysis

Executive summary

In May 2018, ARTICLE 19 analysed Rwanda's 2016 Law Governing Information and Communication Technologies (the Law) for its compliance with international freedom of expression standards.

ARTICLE 19 finds that while the Law purports to provide a regulatory framework, in reality it fails to comply with international human rights standards. The most onerous provisions include the following issues:

- Content-based criminal penalties including criminal defamation, requirements for services to facilitate government surveillance, and sweeping powers to interrupt or suspend any private communications that are "detrimental to the national sovereignty". The Law also harshly restricts content online on illegitimate grounds such as being "indecent" or causing "annoyance" or "anxiety";
- The Law subjects too many services to licensing requirements: it includes the requirement of government licenses in order to provide any electronic communications service;
- The Law imposes overbroad license granting and revocation standards on intermediaries, including broad powers to revoke those licenses for a range of reasons including being "engaged in" or "supporting activities amounting to treason";
- It forces intermediaries to "equip" their services with "technical instruments" to aid in government monitoring of users;
- The Law grants sweeping search and surveillance powers to regulators without judicial or independent oversight and provides broad authority to shut down communications and Internet use;
- The Regulatory Authority, created under the Law, is not an independent entity: it is subjected to government control and is not established by an open and democratic process. The lack of independence of the Regulatory Authority raises great concern because the Authority is granted such significant powers under the Law, including the ability to grant and deny licenses, virtually at will, to almost any service provider in a broad array of sectors including electronic communications; and
- The Law also introduces steep fines of up to 50 million Rwandan francs to enforce technical and regulatory violations. These fines, combined with the breadth of the underlying law, could have a chilling effect on smaller independent media outlets and intermediaries.

We particularly note that ARTICLE 19 is concerned about the impact these provisions will have on freedom of expression in Rwanda. We therefore urge the Rwandan Government to review the Law and bring it into full compliance with international human rights standards.

Summary of recommendations

- Article 22, 60, 126 and 206 should be stricken in their entirety;
- The Law should be amended to explicitly require standards for the members of the Regulatory Authority, namely that they be appointed through an open and democratic process. The members should hold relevant expertise, be independent from political parties and commercial interests, and represent society and civil society as a whole;
- Article 40 should be amended to limit the licensing scheme for electronic communications to cases where public regulation is justified, such as for regulation of the frequency spectrum or regulation of public works;

- Articles 44, 51, and 53 (granting and revoking electronic communications licenses) as well as Article 48 (revoking radio licenses) and Articles 227 and 233 (granting and revoking broadcast licenses) should be amended to stipulate the licensing process in law rather than making it subject to the Regulatory Authority. This should include clear eligibility requirements, clear licensing and renewal policies, and objective assessment criteria;
- Article 51 should be amended, at a minimum, to remove item 7 allowing revocation of a license if the licensee is "engaged in" or "supporting activities amounting to treason";
- Article 53 should be amended to require the Regulatory Authority to provide reasons for suspending a license. It should also be amended to remove items 1 and 3 which allow license suspensions on vague grounds of "national security" and adversely affecting competition;
- The Regulatory Authority should be required to give written reasons for refusing to grant or renew a license, and these decisions should be subject to independent judicial review;
- Restrictions to the import, manufacture, and commerce of communication equipment promulgated under Article 72 should be limited to maintaining technical standards to ensure efficient network operations;
- Articles 33 and 180 as written grant wide warrantless search, entry, and seizure powers to the Regulatory Authority and any individuals it designates. The provisions should be stricken in their entirety. Searches and seizures must be subject to independent judicial review and require cause;
- Article 123 should be stricken. It imposes active obligations on providers to provide potentially limitless government access to user data, and threatens to undermine encryption services which are integral to the realization of freedom of expression and privacy online;
- Computer crimes should be stricken from the Law and dealt with using separate legislation. At a minimum, criminal offenses should have clear intentionality requirements and require "dishonest intent" and "serious" harm to result; and
- Article 197 should include a public interest defence.

Table of contents

Introduction

In this legal analysis, ARTICLE 19 reviews the 2016 Law Governing Information and Communication Technologies in Rwanda, Law No 24/2016 of 18 June 2016 (the Law) for its compliance with international freedom of expression standards. ARTICLE 19 finds that the Law largely fails to meet the relevant standards and should be urgently reviewed.

The digital industry in Rwanda has grown at an accelerated pace over the past ten years, with the country undergoing a "technology revolution" in 2016; while mobile technology has encouraged a new generation of Rwandan entrepreneurs. Against this backdrop the Rwandan Parliament adopted a new regulatory framework in 2016 to cover electronic communications, information communication technologies companies, and other sectors including broadcast, radio, and the postal service. The Law was adopted as a part of this process.

Additionally, ARTICLE 19 believes that the problematic aspects of the Law are even more serious in the light of increasing restrictions on online freedom of expression in Rwanda.[1] ARTICLE 19 notes that in recent years many independent media outlets and opposition blogs have been blocked, and journalists have reported receiving threats to delete content or have their websites shut down.[2] In 2017, ARTICLE 19 expressed concern over regulations passed by the National Electoral Commission (NEC) requiring presidential candidates in the August 2017 elections to seek approval of campaign messages posted online.[3] In a positive response, the Rwanda Utilities Regulatory Authority (RURA) declared that the NEC had no mandate to regulate social media.[4] Such responses are a positive step but ultimately do not remedy underlying legislation that enables severe restrictions on freedom of expression.

Telecommunications are currently a central issue in Rwanda which has seen unprecedented expansion in this sector and is a leader in the industry in East Africa. However, we believe that it is vital that Rwanda's efforts to regulate these issues are consistent with its obligations to protect and promote freedom of expression under international law.

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

[1] See, e.g. ARTICLE 19, Rwanda: ARTICLE 19 Delivers UPR Outcome Statement, UN Human Rights Council, 31st session, 16 March 2015; Rwanda Civil Society Coalition on UPR, Mid-Term Assessment Report of the Implementation of 2015 UPR Recommendations by the Republic of Rwanda, January 2018, pp 10-11.

[2] For example, in 2016 and 2017 many independent media outlets and opposition blogs in Rwanda have been blocked, including *Inyenyeri News*, *The Rwandan*, and *Le Prophete*. Journalists from outlets such as *igihe.com* and *Kihali Today* have reported receiving calls by authorities to delete content criticizing government officials, while other online news websites have reported receiving threats to delete content or be blocked. Several Rwandan journalists have been arrested and charged in recent years with criminal offenses, including Joseph Nkusi, Shyaka Kanuma, and Violette Uwamahoro. See, Freedom House, Rwanda: Country Profile, Freedom on the Net 2017; A. Gagwa, A study of Internet-based information controls in Rwanda, Centre for Intellectual Property and Information Technology Law, Strathmore Law School, Kenya, October 2017.

[3] Under the rule, candidates were required to get campaign messages (including through social media) approved by the NEC 24 hours in advance. The Executive Secretary of the NEC said that the reasoning behind the rule was to make sure that campaign messages were not "poisoning the minds" of Rwandans. See, ARTICLE 19, Rwanda: National Election Commission to censor candidates' online campaign messages, 11 October 2017.

[4] A. Kulamba, Statement by Rwanda Utilities Regulatory Authority (RURA), 31 May 2017.

out key recommendations at the end of each section.

ARTICLE 19 urges the Rwandan Government and the Parliament to address the shortcomings identified in this analysis to ensure the compatibility of the Law with international standards of freedom of expression. We stand ready to provide further assistance in this process.

International human rights standards

ARTICLE 19's comments on the Law are informed by international human rights law and standards. The Law should also comply with the guarantees of freedom of expression in the Rwandan Constitution.[5]

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, in particular Article 19 of the **Universal Declaration of Human Rights (UDHR)**[6] and Article 19 of the **International Covenant on Civil and Political Rights (ICCPR)**[7] as well as in Article 9 of the African Charter on Human and Peoples' Rights.[8] Additional guarantees to freedom of expression are provided in the 2002 Declaration of Principles on Freedom of Expression in Africa (African Declaration).[9]

Importantly, **General Comment No 34**[10] explicitly recognises that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[11] State parties to the ICCPR are also required to consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[12] 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.[13]

Similarly, the four special mandates for the protection of freedom of expression have highlighted in their **Joint Declaration on Freedom of Expression and the Internet** of June 2011 that the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary.[14]

Limitations on the right to freedom of expression

Under international standards, restrictions on the right to freedom of expression must meet the conditions of so called "three-part test" which mandates that restrictions must:

---

[5] Article 38 of the 2003 Constitution of Rwanda guarantees freedom of expression and freedom of access to information where it does not prejudice public order, good morals, the protection of the youth and children, the right of every citizen to honour and dignity and protection of personal and family privacy.
[6] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[7] GA Resolution 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[8] CAB/LEG/67/3 rev. 5 I.L.M. 58 (1982).
[9] Adopted at the 32nd Session of the African Commission on Human and Peoples' Rights, 17-23 October 2002, Article II.
[10] Human Rights Committee (HR Committee), CCPR/C/GC/3, adopted on 12 September 2011.
[11] *Ibid*, para 12.
[12] *Ibid*, para.17.
[13] *Ibid*, para. 39.
[14] Joint Declaration on Freedom of Expression and the Internet, June 2011.

- **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 least restrictive measure must be applied.[15]

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[16]

Additionally, 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. At the same time, inciting violence is more than just expressing views that people disapprove of or find offensive.[17] At the international level, the UN has developed the Rabat Plan of Action which provides the closest definition of what constitutes incitement law under Article 20(2) ICCPR.[18]

Online content regulation

In addition to the above outlined standards, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) in his September 2011 report, clarified the scope of legitimate restrictions on different types of expression online.[19] He identified three different types of expression for the purposes of online regulation:

- Expression that constitutes an offence under international law and can be prosecuted criminally.[20] 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;[21]

- Expression that is not criminally punishable but may justify a restriction and a civil suit; and

- Expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[22]

---

[15] HR Committee, *elichkin v. Belarus*, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).
[16] General Comment 34, *op.cit.*, para. 43.
[17] *C.f.* European Court, *Handyside v the UK*, judgment of 6 July 1976, para. 56.
[18] See UN Rabat Plan of Action (2012). In particular, it clarifies that regard should be had to six part test in assessing whether speech should be criminalised by states as incitement.
[19] Report of the Special Rapporteur on FOE, A/66/290, 10 August 2011, para 18.
[20] *Ibid.* The Special Rapporteur clarified that the only exceptional types of expression here are child pornography, direct and public incitement to commit genocide, hate speech; and incitement to terrorism.
[21] *Ibid*, para. 22.
[22] *Ibid.*

In his 2016 report on freedom of expression in the private sector, the Special Rapporteur on FOE reiterated the need in the communication technology context for any demands, requests, or similar measures related to the take down of content or accessing customer information to satisfy the three-part test under ICCPR Article 19(3).[23] He emphasized that states should set out to transparently implement regulations and policies. He also observed that service shutdowns are a "particularly pernicious means of enforcing content regulations."[24]

Independence of the regulatory body

The guarantee of freedom of expression applies with particular force to the media. The need for protection of regulatory bodies against political or commercial interference was specifically emphasised in the 2003 Joint Declaration of freedom of expression mandates, who considered:

> All public authorities which exercise formal regulatory powers over the media should be protected against interference, particularly of a political or economic nature, including by an appointments process for members which is transparent, allows for public input and is not controlled by any particular political party.[25]

Guaranteeing the independence of a regulator in practice involves various aspects. For instance, **the Access to the Airwaves: Principles on Freedom of Expression and Broadcast Regulation[26]** highlight that:

> [The] institutional autonomy and independence of broadcast and/or telecommunications [regulatory bodies] should be guaranteed and protected by law, including in the following ways:
> - specifically and explicitly in the legislation which establishes the body and, if possible, also in the constitution;
> - by a clear legislative statement of overall broadcast policy, as well as of the powers and responsibilities of the regulatory body;
> - through the rules relating to membership;
> - by formal accountability to the public through a multi-party body; and
> - in funding arrangements.

Media pluralism

Under international law, States are required to promote media pluralism. In this connection, the establishment of an independent regulator is a key to ensuring plurality and diversity. This was confirmed by freedom of expression mandates in the 2007 Joint Declaration on Promoting Diversity in the Broadcast Media, which stated:

> Regulation of the media to promote diversity, including governance of public media, is legitimate only if it is undertaken by a body which is protected against political and other

[23] Report of the Special Rapporteur on FOE, A/HRC/32/38, 11 May 2016, para. 85.
[24] *Ibid*, para. 48.
[25] The 2003 Joint Declaration, the UN Special Rapporteur on Freedom of Expression, the OAS Special Rapporteur on Freedom of Expression and the OSCE Special Representative on Freedom of the Media, 18 December 2003.
[26] ARTICLE 19, Access to the Airwaves Principles on Freedom of Expression and Broadcast Regulation, London, March 2002.

> forms of unwarranted interference, in accordance with international human rights standards.[27]

Other aspects of the promotion of pluralism include equitable access to the airwaves; fair and transparent licensing processes; and the prevention of undue media ownership concentration.

The right to privacy, and surveillance of communications

The right to privacy[28] complements and reinforces the right to freedom of expression as it is essential for ensuring that individuals are able to freely express themselves, including anonymously,[29] should they so choose. The mass-surveillance of online communications therefore poses significant concerns for both rights.

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test.[30] In terms of surveillance (within the context of terrorism in this instance), he defined the parameters of the scope of legitimate restrictions on the right to privacy in the following terms:

> States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on the showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.[31]

The Special Rapporteur on FOE has also observed that:

> The right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of the administration of criminal justice, prevention of crime or combatting terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of

[27] The 2007 Joint Declaration on Diversity in Broadcasting, the UN Special Rapporteur on FOE, the OAS Special Rapporteur on Freedom of Expression, the OSCE Special Representative on Freedom of the Media and the ACHPR (Special Rapporteur on Freedom of Expression and Access to Information, 12 December 2007.
[28] Article 17 of the ICCPR states: "1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2) Everyone has the right to the protection of the law against such interference or attacks." In **General Comment no. 16** on the right to privacy, the HR Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives the ICCPR. See HR Committee, General Comment 16, 23rd session, 1988, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).
[29] *Ibid*, para. 84.
[30] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009, para. 17.
[31] *Ibid.*, para. 21.

protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.[32]

Anonymity and encryption

The protection of anonymity is a vital component in protecting the right to freedom of expression as well as other human rights, in particular the right to privacy. A fundamental feature enabling anonymity online is encryption.[33] Without the authentication techniques derived from encryption, secure online transactions and communication would be impossible.

Traditionally, the protection of anonymity online has been linked to the protection of the right to privacy and personal data. In May 2015, the Special Rapporteur on FOE, published his report on encryption and anonymity in the digital age.[34] The report highlighted the following issues in particular:

- 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;[35]

- 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.[36]

- Restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.[37] 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. 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.[38]

The Special Rapporteur's report also addressed compelled 'key disclosure' or 'decryption' orders whereby a government may "force corporations to cooperate with governments, creating serious challenges that implicate individual users online."[39] The report stipulated that such orders should be

- based on publicly accessible law;
- clearly limited in scope focused on a specific target;
- implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets; and
- only adopted when necessary and when less intrusive means of investigation are not

[32] The May 2011 Report of the UN Special Rapporteur on FOE, *op.cit.*, para. 59.
[33] Encryption is a mathematical "process of converting messages, information, or data into a form unreadable by anyone except the intended recipient" that protects the confidentiality of content against third-party access or manipulation; see e.g. SANS Institute, History of encryption, 2001.
[34] Report of the Special Rapporteur on FOE, A/HRC/29/32, 22 May 2015.
[35] *Ibid,* paras 12,16 and 56.
[36] *Ibid,* para. 53.
[37] *Ibid,* para. 56.
[38] *Ibid,* paras 31-35.
[39] *Ibid.*, para. 45.

available.[40]

Cybercrime

No international standard on cybercrime exists in the area.

From the regional standards, the 2001 Council of Europe Convention on Cybercrime (the Cybercrime Convention) has been the most relevant standard.[41] Although Rwanda is not a signatory to the Convention, it provides a helpful model for states seeking to develop cybercrime legislation. The Cybercrime Convention provides definitions for relevant terms, including definitions for: computer data, computer systems, traffic data and service providers. It requires State parties to create offences against the confidentiality, integrity and availability of computer systems and computer data; computer-related offences including forgery and fraud; and content-related offences such as the criminalisation of child pornography. The Cybercrime Convention then sets out a number of procedural requirements for the investigation and prosecution of cybercrimes, including preservation orders, production orders and the search and seizure of computer data.

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

ARTICLE 19 also notes that the 2014 African Union Convention on Cyber Security and Personal Data Protection (African Union Convention)[42] stresses the importance of protecting fundamental rights including the right to freedom of expression. Article 25 requires states enacting cyber security laws to ensure that such laws protect freedom of expression and adhere to regional conventions such as the African Charter on Human and Peoples' Rights. However, ARTICLE 19's view is that the criminal penalties and content-based regulations present in the Convention fall short of the standards of permissible limitations on freedom of expression under other binding instruments to which Kenya is a party. The analysis will point out such discrepancies where appropriate.

Namely, the African Union Convention does not require "dishonest" intent or "serious" harm for offences; nor does it provide for public interest defences for offences. Most problematically, the African Union Convention undertakes to criminalise several content-related offences. Some of these offences, including production or publication of child pornography, achieve legitimate ends that are consistent with permissible restrictions under Kenya's international human rights obligations. However, others, such as punishing insults based on political opinion, are overbroad and would proscribe expression that does not arise to illegitimate speech.

[40] *Ibid.*
[41] The Council of Europe Convention on Cybercrime, CETS No. 185, in force since July 2004. As of May 2015, 46 states have ratified the Convention and a further eight states have signed the Convention but have not ratified it.
[42] The 2014 African Union Convention on Cyber Security and Personal Data Protection, adopted on 27 June 2014.

Analysis of the Law

General Comments

Before laying down our specific concerns, ARTICLE 19 would like to make the following key observations regarding the Law. In doing so we emphasize that intermediaries, including Internet Service Providers (ISPs), search engines, social media platforms, and web hosts, play a crucial role in accessing and expressing information via electronic means including the Internet. We find that restrictions on intermediaries tend to have a chilling effect on freedom of expression, as we observe that intermediaries tend to err on the side of caution by over-censoring potentially unlawful content.

- **The Law creates broad powers to interrupt or shut down electronic intermediaries and communications without prior judicial authorization or exceptional cause:** In particular, Articles 22 and 126 provide the Information and Communication Technologies) Minister, a government appointee, the ability to issue suspension or interruption orders to providers and also direct the Regulatory Authority to do so. These powers are allowed for a range of reasons, including if the ICT Minister determines that a communication "appears detrimental to the national sovereignty." This is a subjective and potentially limitless standard. We note that under international standards, "Internet shutdowns" - cutting off Internet access, or even access to parts of the Internet for either the whole population or part of the population - is a disproportionate interference with the right to freedom of expression. Shutdowns can never be justified on either public order or national security grounds. Measures such as mandatory blocking of access to websites, IP addresses, ports, network protocols or types of uses should only be ordered by a court or an independent and impartial adjudicatory bodies;

- **The Law creates several content-based offenses** that are vague and overbroad and do not meet the components of the three-part test under international law, particularly the test of legality. It also creates criminal offences which should be considered in separate legislation, not in a telecommunications regulatory law;

- **The Law lacks an independent regulatory body:** Article 10 of the Law establishes a Regulatory Authority that is supposed to be "independent;" however, despite declaring that the Authority is independent, the Law makes no further effort to actually ensure the independence of the Authority or describe what makes it so. In actuality some provisions of the Law subordinate the Regulatory Authority to decisions of the ICT Minister, a government appointee;

- **The Law lacks procedural safeguards for human rights protections:** There is no reference to Rwanda's obligations to uphold and protect the right to freedom of expression and other human rights protected by international law. The absence of any such provisions could threaten the entire Law's compatibility with international standards and the enforcement of human rights in this area.

Content restrictions

As already noted above, ARTICLE 19 is concerned that the Law creates several content-based

offenses that are vague and overbroad. These include:

- **Article 60** which prohibits *inter alia* sending messages by means of a public electronic communications network that are "grossly offensive," or "of indecent obscene or menacing character," or "false" or "persistently using public electronic communications network for purposes of causing annoyance, inconvenience, or needless anxiety";
- **Article 206** which provides a criminal penalty for anyone who "causes to be published in electronic form, any indecent information".

ARTICLE 19 notes that these terms are unacceptably vague. We reiterate that restrictions on freedom of expression must serve a legitimate legislative objective which is of sufficient importance to justify limiting a fundamental right. We make the following observations:

- The term "**grossly offensive**" is not defined. In any case, we note that the right to freedom of expression has long been interpreted as being applicable not only to information or ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that "offend, shock or disturb";[43]

- As for the restrictions of content on the basis of "**obscenity**", in order to determine whether these are justified, it is necessary to examine a number of important factors, including whether there has been an effort to distinguish 'offensive' material from material that is actually harmful (i.e. to children); and how the protection of children has been addressed. Courts in many jurisdictions have distinguished 'offensive' material from material that is actually harmful, only allowing restrictions which have as their objective the prevention of harm. Historically, States have often been guilty of a form of paternalism in applying restrictions on sexually explicit material. Such paternalism is inconsistent with human rights guarantees, including freedom of expression, which presume that all adults are equal and responsible moral agents. It is not for a judge, or even elected officials, to decide what materials we should or should not be able to access, in the absence of a real risk of actual harm;

- We also note that the **falsity of information** is not a legitimate basis for restricting expression under international human rights law. As outlined above, international and regional freedom of expression mandates have stated that "general prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information', are incompatible with international standards for restrictions on freedom of expression."[44]

- Restricting expression on any medium because it causes inconvenience or "anxiety" is an incredibly vague and potentially limitless standard. It does not meet the test of legality to adequately put individuals on notice of what conduct is restricted.

Recommendations

- Article 60 and 206 should be stricken in their entirety.

[43] *C.f. Handyside v the UK*, *op.cit.*
[44] 2017 Joint Declaration, *op. cit.*

The Regulatory Authority

Article 8 provides for the creation of the Regulatory Authority – an authority in charge of ICT policymaking as well as a regulatory body. While Article 10 provides that this Regulatory Authority be independent, the independence appears to be assumed without providing specifics as to how that independence is ensured. In some cases, the Regulatory Authority is subordinate to the ICT Minister, a government appointee (see Article 22, discussed below).

The assumption of independence of the authority also appears in the Explanatory Memorandum of the Law, where the Rwandan Parliament indicated that the 2016 Law included elements to ensure that the authority is "accountable and objective" and that the Law guarantees "the independence of the regulatory Authority in its relation to the political authorities."[45] The elements mentioned include creating a transparent consultation process with sector players, publication of annual reports, and publication of decisions.

However, these measures do not address the actual composition or *independence* of the Regulatory Authority. The Law does not prevent the determinations of the Authority from being subject to government approval and there is no express language stopping the Authority from being subordinate to the executive. For instance, Article 22 gives the ICT Minister the "power to direct the Regulatory Authority to issue to any person a direction suspending or restricting" rights to provide ICT services; thus the Regulatory Authority is expressly subordinate to the ICT Minister, a government appointee.

There are no standards for the composition of the Authority.

ARTICLE 19 reiterates that under international standards regulatory bodies should enjoy operational and administrative autonomy which shall be respected at all times. There is no particular wording prescribed as for this, however, explicitly stipulated guarantees of independence include the functional, operational and administrative autonomy. Moreover, the procedures for appointments of the regulatory bodies should be transparent in accord with international standards. The members of the regulatory bodies should be appointed through an open and democratic process, be representative of society as a whole, and possess relevant expertise.

Recommendation

- The Law (including Article 10) should be amended to explicitly require standards for the members of the Regulatory Authority, namely that they be appointed through an open and democratic process. The members should hold relevant expertise, be independent from political parties and commercial interests, and represent society and civil society as a whole.

Overbroad licensing requirements

The Law grants the Regulatory Authority very broad and non-transparent power in whether or not to grant licenses, and also subjects virtually any entity remotely connected to Internet or communication technology to strict prior authorization requirements before operating. Further, licenses can be suspended for a variety of reasons.

[45] See Republic of Rwanda, Parliament, Explanatory Memorandum to the ICT Bill.

Large number of services are subject to licensing

Article 40 outlines four categories of electronic communications fields subject to licensing. Some of the categories are broadly defined as to cover services that may not apply to broadcast or broadband spectrums, i.e. covering any entities that "provide services to those using electronic communications networks" or "electronic data storage, internet access services as well as other information transfer services." Since "electronic communications networks" as defined in Article 3 cover a vast range of any means of distributing information over an electronic medium, this requires virtually any Internet providers or any associated business to apply for licenses.

ARTICLE 19 finds these provisions is too broad. Licensing schemes should be limited to instances where there is a need for public regulation, such as regulating the frequency spectrum. This does include Internet- or data-related services. Article 40 should only apply to regulating sectors where resource scarcity (such as a frequency spectrum) is at issue.

Grounds for granting and suspending licenses are too broad

Several provisions pertaining to the grant and suspension of licenses are problematic. These include the following:

- Article 44 provides "special criteria" for the grant of these licenses to be dependent on vague factors that are up to the sole determination of the Regulatory Authority. The Regulatory Authority can deny a license if it has a "justifiable reason to suspect that the applicant will violate the provisions of this Law or other laws" or "justifiable elements to suspect that the activity of the applicant would endanger the state security or public order";

- Under Article 53 the Authority can deny licenses on grounds of "national integrity" or "national security" as well as if competition in the electronic communications sector will be "adversely affected";

- The Regulatory Authority is not required to provide reasons for denying a license under the aforementioned grounds. Article 44 provides that the reason for denials related to state security or public order "may not be disclosed to the applicant". Article 53 says the Authority does not have to provide reasons for denying a license if the grounds involve national security;

- Article 51 allows for the immediate suspension of a license if the Authority determines that the licensee is "supporting activities amounting to treason";

- Later provisions such as Article 48 allow cancellation of a radio license if it is used in an "inappropriate way due to its technical characteristics" while Article 227 allow the Regulatory Authority to refuse to grant a broadcasting license on "legal or security grounds";

- Pursuant to Article 233 the Authority can revoke a broadcasting license "anytime" the Authority "deems it necessary."

We comment further on the licensing requirements for electronic communications services under Articles 44, 51, and 53 which we find problematic for numerous reasons:

- First, the reasons they provide for issuing and revoking licenses are vague and subjective and therefore do not meet the test of legality to put potential licensees on notice of the

requirements for obtaining licenses. For instance, a license may be denied on mere suspicion that an applicant "may" violate any law in Rwanda at some future time. Other provisions such as affecting "national integrity" or 'adversely affecting competition' are similarly broad;

- Second, the reasons provided are not legitimate restrictions under international law. The provision on revoking a license based on a hypothetical 'future' violation of law denies the applicant due process or presumption of innocence. It does not even require the applicant to commit actual wrongdoing yet alone be convicted by a court of law. We also note that several of the standards including supporting activities "amount to treason" are not legitimate restrictions of freedom of expression;

- Third, the provisions of above articles do not provide sufficient transparency, and Articles 44 and 53 specifically exempt the Regulatory Authority from providing the reasons for its decisions. The Law should provide that the Authority clearly state its reasons for granting, denying, or revoking licenses;

- Fourth, the Law should make available independent judicial review for these decisions;

- Fifth, the lack of independence of the Regulatory Authority (discussed previously) makes the determinations of issuing licenses subject to political considerations.

The grounds for issuing and revoking licenses in the broadcast and radio context are problematic, as they grant sweeping authority to the Regulatory Authority without articulating the standards for licenses in law. While we acknowledge that the legislative process may not be the ideal medium for implementing detailed rules of technical complexity, the Law should at least specify primary rules and principles needed to obtain a license.

Recommendations

- Article 40 should be amended to limit the licensing scheme for electronic communications to cases where public regulation is justified, such as for regulation of the frequency spectrum or regulation of public works;
- Articles 44, 51, and 53 (granting and revoking electronic communications licenses) as well as Article 48 (revoking radio licenses) and Articles 227 and 233 (granting and revoking broadcast licenses) should be amended to stipulate the licensing process in law rather than making it subject to the Regulatory Authority. This should include clear eligibility requirements, clear licensing and renewal policies, and objective assessment criteria;
- Article 51 should be amended, at a minimum, to remove item 7 allowing revocation of a license if the licensee is "engaged in" or "supporting activities amounting to treason;"
- Article 53 should be amended to require the Regulatory Authority to provide reasons for suspending a license. It should also be amended to remove items 1 and 3 which allow license suspensions on vague grounds of "national security" and adversely affecting competition;
- The Regulatory Authority should be required to give written reasons for refusing to grant or renew a license, and these decisions should be subject to independent judicial review.

Access to technology

Article 72 gives the Regulatory Authority the power to publish technical standards; and Article 288 provides large penalties of 2 to 5 million Rwandan francs and license suspensions for non-

compliance. Article 62 bars the import or sale of equipment that does not comply with these technical standards, and Article 64 can be used to designate specific types of equipment that require advance approval by the Regulatory Authority.

The ability to use technological equipment is part of the exercise of freedom of expression. We note that it may be necessary to restrict the trade of certain telecommunications equipment to ensure compliance with technical standards. However, we insist that any limitations on acquiring technology or using networks or services be compatible with the three-part test under international law.

Recommendation

- Restrictions to the import, manufacture, and commerce of communication equipment promulgated under Article 72 should be limited to maintaining technical standards to ensure efficient network operations.

Search, seizure, and surveillance powers

The Law introduces a number of search, seizure, and surveillance measures that are subject to abuse. We are concerned by these provisions because there is a strong connection between privacy and freedom of expression. Far-reaching search powers have a chilling effect on the ability of individuals and media to engage in free speech.

Some of the most problematic provisions are as follows:

- **Article 123** provides the government the ability to intercept and monitor communications. Specifically, it imposes an obligation on all service providers and electronic communications networks to "equip" their services "with technical instruments and features that allow and facilitate the lawful interception of electronic communications and monitoring." These provisions are problematic for three reasons:
    - First, it creates a vague standard for providers to actively "facilitate" government collection of data which is not defined with enough precision to provide adequate safeguards for the privacy of communications. There is no description of what these technical features entail, and whether they may include the installation of malicious software (malware) on networks. This concern is not without precedent; for instance, reports in 2015 revealed that the government of Rwanda sought to purchase sophisticated malware and other surveillance tools from an Italian-based hacking firm;[46]

    - Second, mandating the installation of interception tools threatens the realization of freedom of expression through the use of encryption. The protection of anonymity is a vital component in protecting the right to freedom of expression as well as other human rights, in particular the right to privacy. In the case of encryption, providers may be unable to furnish communications to the government. Article 123 may threaten providers of anonymity or encryption technologies with penalties for failing to cooperate with providing information if they are unable to decrypt data or communications. The Special Rapporteur on FOE has held that compelled decryption orders are restrictions on expression and hence are subject to the three-part test under international law;

[46] Mari Bastashevski, We Met With Hacking Team in Milan, Motherboard, 11 July 2015.

- Third, requiring operators to install so-called 'backdoors' that allow for circumvention of encryption measures would have the effect of introducing vulnerabilities into services.[47] This would contradict the provision of Article 125 that requires operators to keep networks fully secure.

- **Article 33** allows a judicial police officer, if the Regulatory Authority has "reasonable grounds" for believing a number of suspicions, including that electronic equipment is of a type "not approved by the Regulatory Authority," to "enter and inspect any place" where a service is provided as well as "seize any electronic communication system or equipment" used "in connection with" the communication. With respect to radio communications, the officer may enter "any place in the country" or "stop or board any vessel, aircraft or vehicle" and seize any equipment used in connection with communications. **Article 180** provides the Regulatory Authority or any "authorized officer" the ability to enter, at will, and search and obtain data from any computer system in any business place providing electronic certification services. The Article further imposes active obligations on the administrators or business owners to provide assistance.

  ARTICLE 19 notes that the search and seizure powers provided in these provisions are disproportionate and far exceed the bounds of due process. Article 33 grants broad search and seizure powers without a requirement for judicial authorization and based on "reasonable grounds" rather than "probable cause". Article 33's grant of power to board any vessel or vehicle in the country is limitless jurisdiction without court oversight. Article 180 provides the power for the Regulatory Authority or any appointed person to search and seize places and materials – not necessarily related to telecommunications services – without any judicial authorization or cause. Any search and seizure powers should at a minimum be defined in law and subject to independent judicial review.

Recommendations

- Articles 33 and 180 as written grant wide warrantless search, entry, and seizure powers to the Regulatory Authority and any individuals it designates. The provisions should be stricken in their entirety. Searches and seizures must be subject to independent judicial review and require cause;
- Article 123 should be stricken. It imposes active obligations on providers to provide potentially limitless government access to user data, and threatens to undermine encryption services which are integral to the realization of freedom of expression and privacy online.

Service interruptions and suspensions without prior judicial authorization or exceptional circumstances

Article 22 provides the Minister to ability to order the Regulatory Authority to issue orders to suspend or restrict any service provider's ability to provide electronic communications services. In addition to the aforementioned issue that this subordinates the Regulatory Authority (which is supposed to be independent) to the ICT Minister, Article 22 provides vague and broad pretexts for allowing such shutdowns. The reasons given are "to protect the public from any threat to

[47] Robby Mook, Encryption keeps us safe. It must not be compromised with 'backdoors', The Guardian, 12 February 2018.

public safety, public health or in the interest of national security".

Further, Article 126 gives the power to "interrupt or cause to be interrupted, any private communication that appears detrimental to the national sovereignty, contrary to any existing law, public order or good morals". The Article also allows the Minister to "suspend wholly or in part any electronic communications service or network" indefinitely.

ARTICLE 19 observes that under international standards, cutting off Internet access in whole or part for any part of the population is a disproportionate interference with the right to freedom of expression. Shutdowns can never be justified on either public order or national security grounds. Measures such as mandatory blocking of access to websites, IP addresses, ports, network protocols or types of uses should only be ordered by a court of law.

As written, the pretext of interrupting a private communication that the government-appointed ICT Minister determines "appears detrimental to the national sovereignty" is not a legitimate restriction of expression. Neither is shutting down or restricting Internet access a proportionate response to promoting public order or safety. As such Articles 22 and 126 fail the three-part test under international law.

In times of genuine emergency, there may be legitimate grounds for authorities to adopt exceptional measures, such as requiring broadcasters to carry emergency announcements. These grounds are already addressed in Article 128 which provides for disaster management plans.

Recommendation

- Articles 22 and 126 should therefore be stricken as being disproportionate. The possibility of cutting off Internet access should be prohibited in its entirety.

Cybercrime offenses

Chapter III, Section 10 of the Law provides several sanctions for cybercrime offences (Articles 197-206). These offenses require minimal or no intent and are repetitive in several parts.

ARTICLE 19 notes that from a comparative perspective, a useful model for drafting cybercrime legislation is the Convention on Cybercrime - the most widely-adopted treaty on computer crimes - which outlines a small number of offences with clear intentionality requirements. ARTICLE 19 observes that the Law is not an appropriate venue for introducing criminal cybercrime sanctions and that any criminal offences should be provided in the Penal Code.

While we recommend that these measures be addressed in separate legislation, we comment on the following issues:

- Several provisions contain minimal or no intentionality requirements, which falls below what is required in the Cybercrime Convention. At a minimum, the provisions in this section should be amended to require "dishonest intent" and "serious" harm to result. For example; Article 197 should include "dishonest intent to gain access or to obtain computer data;"

- Several provisions are repetitive. Articles 198 and 199 repeat Article 197 in terms of creating access offenses. We also note that Articles 204, and 205 create offenses that do not individually appear in the Cybercrime Convention and would be covered by Article 203 on computer-related fraud and an offense pertaining to 'misuse;'

- As noted previously, Article 206 should be stricken as it punishes publication of "indecent" information which is not a legitimate restriction under international law;

- Criminal offenses must specify punishments under law. Chapter III does not indicate what criminal penalties apply, but simply refers to the Penal Code;

- We recommend the availability of a 'public interest defence'. Overbroad cybercrime offenses can punish legitimate disclosures of information, such as disclosure of wrongdoing to journalists in the public interest.

Recommendations

- Computer crimes should be stricken from the Law and dealt with using separate legislation.
- At a minimum, criminal offenses should have clear intentionality requirements and require "dishonest intent" and "serious" harm to result;
- Article 197 should include a public interest defence;
- Several offenses are repetitive and unnecessary, including Articles 198, 199, 204, and 205, which can be dealt with using fewer offenses. The Cybercrime Convention can be used as a reference for this area;
- Article 206 should be stricken as punishing the publication of "indecent information" is not a legitimate restriction of expression under international law;
- Criminal offenses must specify punishments to meet the test of legality; as written, Chapter III, Section 10 refers to criminal penalties in the Penal Code but does not indicate what those penalties are.

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.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org.

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