Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**215**
Land:	Rwanda
Kilde:	ARTICLE 19 og Access Now
Titel:	Joint submission to the Universal Periodic Review of Rwanda by ARTICLE 19 and Access Now
Udgivet:	9. juli 2020
Optaget på baggrundsmaterialet:	7. januar 2021

Joint submission to the Universal Periodic Review of Rwanda by ARTICLE 19 and Access Now

For consideration during the 37th Session of the Working Group

9 July 2020

Executive Summary

1. ARTICLE 19 and Access Now welcome the opportunity to contribute to the third cycle of the Universal Periodic Review (**UPR**) of Rwanda. This submission assesses Rwanda's compliance with its human rights obligations relating to the right to freedom of expression and information, including their intersection with the right to privacy. It considers the following areas of concern:

    - Legal Framework for Free Expression
    - Freedom of Expression Online
    - Media Freedom and Self-Regulation
    - Safety of Journalists
    - Access to Information
    - Privacy and Data Protection
    - Internet Access

2. In the period under review, the Supreme Court struck down restrictive provisions contained in the Penal Code and the government ratified the African Union Convention on Cyber Security and Personal Data Protection (**Malabo Convention)**.[1]

3. However, serious challenges persist, including incompatible criminal defamation and insult provisions, broad surveillance powers, online and offline attacks against journalists, an overly-restrictive regulatory media environment, and the wanting implementation of access to information legislation.

Legal Framework for Free Expression

4. Rwanda accepted recommendations to continue strengthening its legislative framework and eliminate all provisions that undermine freedom of expression.[2]

Constitutional Guarantees for Freedom of Expression

5. Article 38, Constitution of the Republic of Rwanda (2003, revised in 2015)[3] protects the right to freedom of expression.[4] However, this guarantee is not aligned with

1 The African Union (2014) 'African Union Convention on Cyber Security and Personal Data Protection (EX.CL/846 (XXV))'. Available at <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

2 133.1 Continue strengthening its legislation to eliminate all provisions that undermine freedom of expression (Chile); 134.31 Adopt further measures for the protection of political and civil rights (Japan).

3 The Constitution of the Republic of Rwanda (2003, revised in 2015). Available at <https://minijust.gov.rw/fileadmin/Law_and_Regulations/Official_Gazette_no_Special_of_24.12.2015_2_1_.pdf>

4 *Ibid*., Article 38 provides as follows: "*Freedom of press, of expression and of access to information are recognised and guaranteed by the State. Freedom of expression and freedom of access to information shall 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. Conditions for exercising and respect for these freedoms are determined by law."*

international standards, per Article 19(3) of the International Covenant on Civil and Political Rights (or **ICCPR**).[5]

6. Whilst it incorporates the requirement of legality, it fails to articulate the additional, cumulative requirements of legality, necessity, and proportionality, in pursuit of the exhaustive list of recognised grounds for restriction under Article 19(3).[6] The vague and subjective concepts of 'good morals', 'honour and dignity', as well as the 'protection of youth and children' are incompatible with the ICCPR.

Restrictive Provisions in the Penal Code (2018)

7. The revision of the Penal Code (No 68/2018 of 30/08/2018)[7] by Parliament in 2018 introduced restrictive provisions for freedom of expression, in contravention of Rwanda's obligations under international human rights law.

8. In 2018, Advocate Mugisha filed a constitutional petition contesting the constitutionality of various Penal Code provisions.[8] On 24 April 2019, the Supreme Court ruled that various provisions were contrary to Articles 15 and 38, Constitution and repealed Articles 154[9] and 233,[10] revised Penal Code.[11]

---

5 General Assembly (1966) 'International Covenant on Civil and Political Rights, Resolution 2200A (XXI).' Available at <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>

6 These include: national security, public order, public health or morals, and the rights or reputations of others.

7 Law No. 68/2018 of 30/08/2018 Determining offences and penalties in general. Available at <http://www.mhc.gov.rw/index.php?id=5>

8 Re Mugisha [2019] 2 RLR – 2019-01-18 and Re Mugisha [2019] 3 RLR – 2019-04-24. Available at <https://decisia.lexum.com/rlr/en/d/s/index.do?cont=Re+Mugisha&iframe=false&col=72>. The petition was first heard by the Supreme Court on 4 December 2018.

9 Article 154 criminalised '*public defamation of religious rituals*', punishable by between 15 days and 3 months' imprisonment, and a fine of 100,000-200,000 Rwandan Francs (105 - 210 USD). Article 154, Law No. 68/2018 of 30/08/2018 Determining offences and penalties in general. Available at <http://www.mhc.gov.rw/index.php?id=5>

10 Article 233 criminalised the '*humiliation of national authorities and persons in charge of public service*'), punishable by imprisonment of between 1-2 years and a fine of 500,000-1,000,000 Rwandan Francs (525 – 1,051 USD). Aggravated sentences – doubling the available fine and prison term – were applicable to cases involving expression directed to top-ranking authorities, or taking place during sessions of Parliament. Article 233, Law No. 68/2018 of 30/08/2018 Determining offences and penalties in general. Available at <http://www.mhc.gov.rw/index.php?id=5>

11 We note that the repeal of blasphemy and religious insult laws (Article 154) is supported by the Human Rights Committee, recommended in the Office of the High Commissioner on Human Rights-backed Rabat Plan of Action, and by numerous Special Procedures of the United Nations Human Rights Council. Similarly, international standards are clear that public officials, and state institutions (Article 233), should not be subject to heightened protection from criticism, but rather be expected to tolerate heightened scrutiny in light of their public role. See: UN Human Rights Committee 'General Comment No.34: Article 19: Freedoms of opinion and expression' para. 48. Available at <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/ProcessAdoptionDGCArticle9.aspx>; Special Rapporteur on freedom of religion or belief (2017) 'Report of the Special Rapporteur on freedom of religion or belief, A/HRC/34/50.' Available at <https://www.refworld.org/docid/58ad9e924.html>; Special Rapporteur to the Human Rights Council (HRC) and the General Assembly (2016) 'Report of the Special Rapporteur on freedom of expression, A/71/33.' Available at <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx>; Special Rapporteur on Minority Issues (2015) 'Report of the Special Rapporteur on minority issues, A/HRC/28/64.' Available at <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session28/Pages/ListReports.aspx>; UN Working Group on Arbitrary Detention (2008) 'Opinion No. 35/2008 (Egypt), para 38. Available at <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/13/30/Add.1>. The UN Human Rights Council has also been supported by regional mandates, see: UN Special Rapporteur on Freedom of Opinion and Expression,

9. However, we remain concerned about the retention of the following provisions in the Penal Code, one of which was considered and declared 'compatible with Articles 15 and 38 of the Constitution' by the Supreme Court:

- **Article 236:** criminalises '*insults or defamation against the President*', punishable by between 5-7 years' imprisonment, and a fine of between 5 and 7 million Rwandan Francs (5,255 – 7,357 USD). This provision is clearly incompatible with the ICCPR in aiming to shield the President from criticism and inhibiting public debate on political matters of the utmost public interest. Broadly, international standards on freedom of expression are clear that imprisonment is an inherently disproportionate sanction for defamation, with various international and regional human rights mechanisms recommending the repeal of criminal defamation provisions in their entirety.[12]

- **Article 194:** vaguely criminalises the '*spreading (of) false information or harmful propaganda with intent to cause a hostile international opinion against (the) Rwandan Government*.'[13] This carries a stiff maximum penalty of life imprisonment in wartime, and 7 – 10 years' imprisonment in peacetime. The UN and regional mandates on freedom of expression and information have clarified 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."[14]

Recommendation

- Fully protect the right to freedom of expression, online and offline, by repealing Articles 194 and 236 of the revised Penal Code.

Freedom of Expression Online

ICT Law

the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR (African Commission on Human and Peoples' Rights) Special Rapporteur on Freedom of Expression and Access to Information (2008) 'Joint Declaration on defamation of religions, and anti-terrorism, and anti-extremism legislation'. Available at <https://www.osce.org/fom/35639> ;Organization for Security and Co-operation in Europe (2000) 'Joint Declaration - Current Challenges to Media Freedom by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression,' pp. 2. Available at <https://www.osce.org/fom/66176?page=2>

12 The African Court on Human and Peoples' Rights (2013) '*Lohé Issa Konaté v. The Republic of Burkina Faso App. No. 004/2013.'* Available at <https://globalfreedomofexpression.columbia.edu/cases/lohe-issa-konate-v-the-republic-of-burkina-faso>

13 Article 194, Law No. 68/2018 of 30/08/2018 Determining offences and penalties in general. Available at <http://www.mhc.gov.rw/index.php?id=5>

14 Organization for Security and Co-operation in Europe (2017) 'Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda', Declaration 2 (a).' Available at <https://www.osce.org/fom/66176>

10. The ICT Law[15] contains provisions which are substantially incompatible with Rwanda's obligations under the ICCPR and the African Charter on Human and Peoples' Rights (**Charter**),[16] for failing to adhere to proportionality and necessity requirements.[17]

11. ARTICLE 19's legal analysis[18] identified extensive reforms required to ensure the ICT Law compliance with international human rights law and standards, including:

- **Article 22:** empowers the ICT Minister to order the Rwanda Utilities Regulatory Authority (**RURA**) to issue orders to suspend or restrict any service provider's ability to provide electronic communications network or services on vague and broad grounds, including "to protect the public from any threat to public safety, public health or in the interest of national security". It does not provide for judicial oversight or recourse to appeal to prevent possible abuses, and the ICT law generally fails to provide a clear framework regulating the scope of the ICT Minister's powers.

- **Article 60:** broadly and vaguely 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." This section further prohibits "persistently using public electronic communications networks for purposes of causing annoyance, inconvenience, or needless anxiety". Notably, RURA is mandated to 'make and publish instructions for the implementation of this Article', but no rules have been issued yet. Significantly, falsity of information is not a legitimate basis for restricting expression, and restricting expression on the basis of vague concepts such as causing annoyance, or anxiety, or 'indecency', does not conform with the requirements of legality, necessity, or proportionality under Article 19(3).

- **Article 126:** empowers the Minister to "interrupt or cause to be interrupted, any private communication that appears to be detrimental to national sovereignty, contrary to any existing law, public order or good morals." It further provides that the Minister can "suspend wholly or in part any electronic communications service or network", for specified periods or indefinitely. We note that cutting off Internet access in whole or in part, is inherently disproportionate and impedes the enjoyment of a wide range of human rights, including freedom of expression. This was emphasised by the 4 mandate holders on freedom of

---

15 Law Governing ICT, Law No. 24/2016 of 18 June 2016. Available at <http://minict.gov.rw/fileadmin/Documents/Policies_and_Rugulations/ICT_laws/ICT_LAW.pdf>. This law replaced Law No°44/2001 of 30/11/2001 governing telecommunications, Law No° 18/2010 of 12/05/2010 relating to electronic messages, electronic signature and electronic transactions and Decree-Law No° 43/76 of 01/12/1976 on the organisation of the postal service.

16 African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) 1520 UNTS 217 (or **Banjul Charter**). Available at <https://www.achpr.org/legalinstruments/detail?id=49>

17 African Commission on Human and Peoples' Rights (2009) *Zimbabwe Lawyers for Human Rights & Associated Newspapers of Zimbabwe v Republic of Zimbabwe Communication No 284/03,* para 176. Available at <https://globalfreedomofexpression.columbia.edu/cases/zimbabwe-lawyers-human-rights-v-zimbabwe/>

18 ARTICLE 19 (2018) 'Rwanda: 2016 Law Governing Information and Communication Technologies.' Available at <https://www.article19.org/resources/rwanda-law-governing-information-and-communication-technologies/>

expression, in their 2011 Joint Declaration on Freedom of Expression and the Internet.[19]

- **Article 206:** criminalises any person who 'publishes, transmits or causes to be published in electronic form, any indecent information", punishable in accordance with a corresponding offence in the Penal Code. Despite the revised Penal Code being introduced after the ICT Law, the legislative drafters failed to provide a correlating offence in the Penal Code, which subverts rights-holders' need for legal certainty as to the available punishment.

12. The implementation of the ICT Law is overseen by an 'organ in charge of ICT policy making', the ICT Minister, and a 'regulatory organ', RURA.[20] Worryingly, RURA's autonomy is limited. It reports to the Office of the Prime Minister[21] and one of its management organs, the Regulatory Board, consists of 7 members, including the Director General (or **DG**), who are appointed by the President.[22] Freedom House has queried the oversight role played by the "military and intelligence services on the regulation of the ICT sector."[23] The DG role is held on a full-time basis and 2 military officers, Maj. François-Régis Gatarayiha and Patrick Nyirishema, have held this office since 2011.[24]

13. We note that RURA exercised its powers following diplomatic tensions between Rwanda and Uganda. RURA's DG is cited[25] as having consulted with the Uganda Communications Commission regarding RURA's decision to block access to four Ugandan websites, including New Vision, Daily Monitor, Observer and The Independent in August 2019.[26] These four websites, and SoftPower News, 'a Ugandan

---

19 UN Special Rapporteur on Freedom of Opinion and Expression (Special Rapporteur on FOE), the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information (2011) 'Joint Declaration on Freedom of Expression and the Internet', para. 1(a). Available at <https://www.osce.org/fom/78309>

20 Articles 8 – 10, Law No. 09/2013 of 01/03/2013 Establishing Rwanda Utilities Regulatory Authority (RURA) and Determining its Mission, Powers, Organisation and Functioning. Available at <https://rura.rw/fileadmin/docs/report/Official_Gazette_no_14_bis_of_08_04_2013.pdf>. RURA is charged with 'regulating public utilities' including 'telecommunications, information technology, broadcasting, and converging electronic technologies including the Internet and any other audiovisual information and communications technology.' **See:** Article 2, Law No. 09/2013 of 01/03/2013 Establishing Rwanda Utilities Regulatory Authority (RURA) and Determining its Mission, Powers, Organisation and Functioning. Available at <https://rura.rw/fileadmin/docs/report/Official_Gazette_no_14_bis_of_08_04_2013.pdf>

21 Article 11, Law No. 09/2013 of 01/03/2013 Establishing Rwanda Utilities Regulatory Authority (RURA) and Determining its Mission, Powers, Organisation and Functioning. Available at <https://rura.rw/fileadmin/docs/report/Official_Gazette_no_14_bis_of_08_04_2013.pdf>

22 *Ibid.*, Articles 14 & 16.

23 Freedom House (2019) 'Rwanda - Freedom on the Net (2019).' Available at <https://freedomhouse.org/country/rwanda/freedom-net/2019>

24 The New Times (2017) 'President Kagame appoints more leaders.' Available at <https://www.newtimes.co.rw/section/read/219189>

25 The East African (2019) 'Rwanda says Uganda agrees to unblock news sites.' Available at <https://www.theeastafrican.co.ke/news/ea/Rwanda-says-uganda-agrees-to-unblock-news-sites/4552908-5246754-37v5diz/index.html>

26 All Africa (2019) 'East Africa: Two Days after Burying Hatchet, Rwanda and Uganda at it Again.' Available at <https://allafrica.com/stories/201908230735.html>

digital media company' (blocked in January 2018) continue to remain blocked in Rwanda, as at 9 July 2020.[27]

14. We are concerned that offline comments and initiatives risk creating a hostile online environment in Rwanda, especially for ordinary users, journalists, activists and opposition members using online platforms to oppose the government's practices. In 2019, President Kagame issued a warning to opponents that "*those making noise on the Internet do so because they're far from the fire. If they dare get close to it, they'll face its heat*."[28] Additionally, there are reported plans to regulate content generated and shared on social media platforms, ostensibly to curb misinformation. The precise nature of the proposed regulation has yet to be publicly released.[29]

15. In an alarming example of censorship measures by the National Electoral Commission, ARTICLE 19 (2017) expressed concern[30] following the issuance of electoral instructions by the National Electoral Commission.[31] Article 40 required all candidates to seek approval before posting campaign messages online or using electronic means. This provision was repealed[32] and subsequent regulations[33] permit the use of ICT to campaign.

Recommendations

- Fully protect the right to free expression and access to information online by repealing Articles 22, 60, 126, 206, ICT Law to ensure compliance with international human rights law.
- Ensure RURA's practical operation in a free, fair, and autonomous manner.
- Refrain from restricting access to online platforms and illegitimately regulating content disseminated on the Internet.

27 Freedom House (2019) 'Rwanda: Freedom on the Net 2019.' Available at <https://freedomhouse.org/country/rwanda/freedom-net/2019#footnote3_wxrar47>

28 Freedom House (2019) 'Freedom on the net - Rwanda.' Available at <https://freedomhouse.org/country/rwanda/freedom-net/2019>

29 CGTN Africa (2019) 'Rwanda mulling more restrictions on social media'. Available at <https://africa.cgtn.com/2019/05/18/rwanda-mulling-more-restrictions-on-social-media/>

30 ARTICLE 19 (2017) 'Rwanda: National Election Commission to censor candidates' online campaign messages.' Available at <https://www.article19.org/resources/rwanda-national-election-commission-to-censor-candidates-online-campaign-messages/>

31 'Instructions No. 07/2017 of 04/04/2017 of the National Electoral Commission Regulating 2017 Presidential Elections as Modified and Complemented to Date', Official Gazette n°18 bis of 01/05/2017, Article 40 (*repealed*). Available at <http://nec.gov.rw/uploads/media/instructions_on_2017_elections.pdf>.

32 Article 8, Instructions No. 02/2017 of 31/05/2017 of National Electoral Commission. Available at <http://nec.gov.rw/uploads/media/instructions_on_2017_elections.pdf>.

33 This is permitted 'except on websites and social media of public institutions and entities of public interest.'Article 71, Regulations No. 03/2018 of 09/07/2018 of the National Electoral Commission Governing 2018 Parliamentary Elections. Available at <http://www.nec.gov.rw/index.php?id=85>

Media Freedom

16. Rwanda accepted various recommendations to adopt further measures to guarantee freedom of speech and media independence, strengthen and implement the regulatory media policy, including through capacity building of relevant parties and ensure the safety and protection of journalists from harassment and attacks.[34]

Media Law

17. Article 38, Constitution of the Republic of Rwanda protects media freedom.[35] This has been given further effect in the Media Law[36] which fails to comply with international standards on freedom of expression and privacy.

18. Article 2 (19) defines a 'professional journalist' as "a person who possesses basic journalism skills and who exercises journalism as his/her first profession." Journalists are also restricted to various activities.[37] This definition of journalists is restrictive, as it fails to recognise 'citizen journalists', freelance journalists, amongst others. The Rwanda Media Commission (**RMC**) recently issued a statement noting that bloggers availing information on YouTube are not journalists.[38] The Human Rights Committee note that journalism is "a function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the Internet or elsewhere."[39] This definition places a restriction on journalists from self-publishing/broadcasting information outside of state-recognised media organs.[40]

---

34 134.52 Adopt further measures with the aim of guaranteeing freedom of speech and the independence of the media (Cyprus); 133.30 Strengthen efforts in implementing the regulatory media policy to ensure access to information and freedom of opinion and expression, including through capacity-building of relevant parties (Indonesia); 134.55 Step up efforts towards ensuring freedom of expression and the protection of journalists, and seek the assistance, as required, of special procedures, OHCHR and the United Nations Educational, Scientific and Cultural Organization, in order to achieve that end (Brazil); 134.57 Take measures to protect journalists from harassment (Norway); 134.53 Take all necessary measures to protect journalists from harassment and attacks and to ensure that all allegations of violence and intimidation of journalists are promptly and impartially investigated and perpetrators brought to justice (Latvia); 134.54 Take measures to protect journalists from harassment and attacks and ensure independent, credible investigations of alleged cases and the prosecution of offenders (Austria).

35 The Constitution of the Republic of Rwanda (2003, revised in 2015). Available at <https://minijust.gov.rw/fileadmin/Law_and_Regulations/Official_Gazette_no_Special_of_24.12.2015_2___1_.pdf>

36 Law N°02/2013 of 08/02/2013 Regulating Media (Official Gazette No. 10 of 11 March 2013)

37 These include: (a) "collecting information, (b) processing information, © publish/broadcast information through a given media organ with intention to disseminate information or opinions" through a given media organ with intention to disseminate information or opinions.'

38

39 United Nations Human Rights Committee (2011) General Comment No. 34, para 44. Available at <https://digitallibrary.un.org/record/715606?ln=en>

40 Article 2 (5), Law N°02/2013 of 08/02/2013 Regulating Media (Official Gazette No. 10 of 11 March 2013). Available at <http://mhc.gov.rw/fileadmin/user_upload/placeholder/Laws_and_Regulations/Itegeko_Rigenga_Itangazamakuru.pdf>

19. **Article 5** sets out legal duties required of a journalist**.** These include the duty "to inform; to educate (the) population and promote leisure activities; to defend freedom of information and analyse and comment on information."[41] The existence of legal obligations creates a legal responsibility which authorities may use to harass journalists.

20. **Article 9** imposes limits to freedom of opinion and information. Despite the prohibition on censorship, it maintains as follows: "*However, the freedom of opinion and information shall not jeopardize the general public order and good morals, individual's right to honour and reputation in the public eye and to the right to inviolability of a person's private life and family; the freedom shall also be recognized if it is not detrimental to the protection of children*."[42] As noted above, the vague and subjective concepts of 'good morals' and 'honour and reputation' are incompatible with the ICCPR, and impose undue restrictions on the right to freedom of expression.

21. **Article 13:** fails to adequately protect the confidentiality of journalistic sources**.** Here, courts "*may order a journalist to reveal his/her sources of information whenever it is considered necessary for purposes of carrying out investigations or criminal proceedings*."[43] This is applicable to any legal proceedings, rather than mandated for criminal investigations and/or proceedings of a very serious nature. ARTICLE 19[44] noted that Article 13, Media Law does not require courts to establish that there is no other reasonable alternative means available for obtaining information before ordering the disclosure of a source. The UN Special Rapporteur clarified that "journalists should never be forced to reveal their sources except for certain exceptional cases where the interests of investigating a serious crime or protecting the life of other individuals prevail over the possible risk to the source. Such pressing needs must be clearly demonstrated and ordered by an independent court."[45]

Media Self-Regulation

22. There is ongoing ambiguity regarding the roles of multiple media regulators in Rwanda. This has resulted in a duplication of responsibilities and functions and a lack of legal certainty and predictability.

---

41 Article 5, Law N°02/2013 of 08/02/2013 Regulating Media (Official Gazette No. 10 of 11 March 2013). Available at <http://mhc.gov.rw/fileadmin/user_upload/placeholder/Laws_and_Regulations/Itegeko_Rigenga_Itangazamakuru.pdf>

42 Article 9, Law N°02/2013 of 08/02/2013 Regulating Media (Official Gazette No. 10 of 11 March 2013). Available at <http://mhc.gov.rw/fileadmin/user_upload/placeholder/Laws_and_Regulations/Itegeko_Rigenga_Itangazamakuru.pdf>

43 Article 13, Law N°02/2013 of 08/02/2013 Regulating Media (Official Gazette No. 10 of 11 March 2013). Available at <http://mhc.gov.rw/fileadmin/user_upload/placeholder/Laws_and_Regulations/Itegeko_Rigenga_Itangazamakuru.pdf>

44 ARTICLE 19 (2013) 'Rwanda: Media law does not go far enough.' Available at <https://www.refworld.org/docid/5149bdfc2.html>

45 UN Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' A /HRC/20/17, para 109. Available at <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/20/17>

23. Under Article 4, Media Law, RMC is tasked with media regulation.[46] This regulation includes a protective function, and the RMC can receive and address cases of harassment against journalists. However, RURA is also granted regulatory powers over "audio, audio-visual media and internet,"[47] and its media responsibilities are governed by a prime ministerial order[48] under the ICT Law and the Media Law. These two bodies are expected to "have a joint working agreement and shall determine their plan of action."[49]

24. Additionally, 2 other bodies exercise media regulation, including the Rwanda Governance Board (**RGB**) and the Media High Council (**MHC**). The RGB is tasked with the 'promotion of the media sector and the provision of advice on its operations.'[50] The RGB[51] monitors the implementation of (media policy) reforms, collaborates with RMC, RURA and MHC, provides initial funding for the media self-regulatory body and monitors the evaluation of the performance of media houses and associations. On the other hand, MHC is defined as an "independent institution responsible for media capacity building"[52] for journalists, media managers, editors and media outlets.

25. We note that this legislative arrangement - where multiple bodies are tasked with regulation – does not protect media self-regulation, both in theory and in practice. In effect, RMC is unable to function as a genuinely independent, self-regulatory body; this inability is exacerbated by the fact that RMC is not statutorily recognised under the Media Law.[53] In our view, this has resulted in undue influence being exercised over RMC by the Executive.

---

46 Article 4, Media Law provides "*the daily functioning of media and the conduct of journalists shall be regulated by the Media Self Regulatory Body*."

47 Article 4, Law N°02/2013 of 08/02/2013 Regulating Media (Official Gazette No. 10 of 11 March 2013). Available at <http://mhc.gov.rw/fileadmin/user_upload/placeholder/Laws_and_Regulations/Itegeko_Rigenga_Itangazamakuru.pdf>

48 Article 5, *Specific mission of RURA in regard to the media.* Article 2, Law No. 09/2013 of 01/03/2013 Establishing Rwanda Utilities Regulatory Authority (RURA) and Determining its Mission, Powers, Organisation and Functioning. Available at <https://rura.rw/fileadmin/docs/report/Official_Gazette_no_14_bis_of_08_04_2013.pdf>

49 Article 4, Law N°02/2013 of 08/02/2013 Regulating Media (Official Gazette No. 10 of 11 March 2013). Available at <http://mhc.gov.rw/fileadmin/user_upload/placeholder/Laws_and_Regulations/Itegeko_Rigenga_Itangazamakuru.pdf> . An agreement between RMC and RURA was signed in 2013.

50 Article 5, Law N°56/2016 of 16/12/2016 Establishing the Rwanda Governance Board and Determining its Mission, Organisation and Functioning. Available at <https://www.rgb.rw/index.php?id=364>

51 See: Rwanda Governance Board 'Media Coordination and Monitoring Unit.' Available at <https://www.rgb.rw/index.php?id=285>

52 Article 2, Law No 03/2013 of 08/02/2013 Determining the Responsibilities, Organisation, and Functioning of the Media High Council. Available at <mhc.gov.rw/fileadmin/user_upload/placeholder/Laws_and_Regulations/Itegeko_Rigenga_Inama_Nkuru_y_Itangazamakuru.pdf>

53 RMC was unanimously set up following a General Assembly of all Rwandan journalists held on 27/8/2013.

26. Instructively, in February 2015, a Committee of Inquiry (**Committee**) established by RURA, published a report which resulted in an indefinite ban being imposed by RURA on the British Broadcasting Corporation's (**BBC**) Kinyarwanda services on 29 May 2015. This ban followed BBC's airing, on 1 October 2014, of a documentary titled 'Rwanda's Untold Story.' The Committee's report stated that the documentary promoted 'genocide denial, divisionism and incited hatred.'[54] According to RURA, it derived its powers to effect this ban from the law establishing RURA and the Media Law, which "gives it legal powers to act on consumer complaints"[55] as well as a parliamentary resolution passed on 22 October 2014 calling on the government to ban BBC.[56] This ban is still in effect as at 9 July 2020.

27. Reporters without Borders (**RSF**) reported various issues with RURA's ban.[57] Firstly, RSF reports that Fred Muvunyi, former RMC head, challenged RURA's decisions on various grounds. These included RURA's breach of an agreement with RMC and its lack of powers to make determinations on non-technical (*i.e., content*) issues without consulting RMC. Secondly, RMC publicly issued statements which noted that RURA's decision had 'no legal basis.' Lastly, RSF noted that a targeted intimidation campaign was directed towards RMC for challenging RURA's ban.

Safety of Journalists

28. During the previous cycle, Rwanda accepted recommendations to ensure that journalists are protected from harassment and attacks. The government also accepted recommendations to seek the assistance of special procedures, ensure independent and credible investigations for alleged cases and the prosecution of offenders.[58]

29. However, journalists continue to report concerning levels of harassment and intimidation which is enabled by varied restrictive laws, including the Media Law, the revised Penal Code, and the ICT Law.

30. Between 2016 - 2017, the RMC registered 7 cases of harassment and intimidation of journalists. We continue to document other cases, including those identified by other sources. For example:

---

54 Inquiry Committee on the BBC Documentary "Rwanda's Untold Story" (2015) 'Inquiry Committee Report on the BBC Documentary "Rwanda's Untold Story", para 148. Available at <http://rwandabbcinquiry.rw/?page_id=38>

55 The East African (2014) 'Rwanda media agency says BBC ban violates law.' Available at <https://www.theeastafrican.co.ke/news/ea/Rwanda-media-agency-says-BBC-ban-violates-law/4552908-2507644-9whvlv/index.html>

56 RSF (2014) 'BBC's Kinyarwanda broadcasts suspended indefinitely.' Available at <https://rsf.org/en/news/bbcs-kinyarwanda-broadcasts-suspended-indefinitely>

57 RSF (2015) 'What lies behind the indefinite ban on the BBC.' Available at <https://rsf.org/en/news/what-lies-behind-indefinite-ban-bbc>. RSF (2014) 'Rwanda's media self-regulator subjected to intimidation campaign.' Available at <https://rsf.org/en/news/rwandas-media-self-regulator-subjected-intimidation-campaign>

58 134.55 Step up efforts towards ensuring freedom of expression and the protection of journalists, and seek the assistance, as required, of special procedures, OHCHR and the United Nations Educational, Scientific and Cultural Organization, in order to achieve that end (Brazil); 134.57 Take measures to protect journalists from harassment (Norway); 134.54 Take measures to protect journalists from harassment and attacks and ensure independent, credible investigations of alleged cases and the prosecution of offenders (Austria).

- **Media House (2016):** According to reports by human rights organisations,[59] police raided the office of the *East African* newspaper in Kigali. These organisations noted that the police seized material, including hard-copy documents capable of identifying whistleblowers, and confiscated the computers and/or phones of Ivan Mugisha and Johnson Kanamugire, journalists at the newspaper. Human Rights Watch reports that both were 'investigating cases of alleged tax evasion and corruption.' Despite Mugisha not being charged, the police arrested him without an arrest warrant and questioned him in detention for over six hours. It is reported that Johnson was not arrested, due to his absence from the *East African* office. It is widely considered that this raid and Mugisha's subsequent arrest is an example of the government's exertion of pressure on a private media house, and its journalists, for their investigative journalistic work.

- **Investigative Journalists (2018 - 2019):** ARTICLE 19 notes that four investigative journalists – two freelancers and two journalists working for media houses - relocated from Rwanda between 2018 - 2019. These four journalists were working on a security story detailing border security tensions between Rwanda and Uganda and a corruption story seeking to uncover police officers' facilitation of drug smuggling into Rwanda. Despite two journalists relocating back to Rwanda, the other two continue to work in exile. We note that the number of exiled Rwandan journalists is likely to be higher, as under-reporting due to fears of reprisal is a widespread problem.

Recommendations

- Amend Articles 2(19), 5, 8 and 13 of the Media Law and ensure that it complies with international standards on freedom of expression.
- Promote media self-regulation and grant RMC sole media regulation powers by amending the Media Law, and revoke all media powers bestowed on RURA, MHC and RGB.
- Take the necessary measures to stop harassment and attacks against journalists, and conduct impartial, effective and thorough investigations into all violations.

59 Human Rights Watch (2017) 'Chronology of Rwanda's Closing Space.' Available at <https://www.hrw.org/sites/default/files/supporting_resources/rwanda_chronology_2016_2017_english.pdf>; Reporters without Borders (2016) 'Investigative reporter freed provisionally after prosecutor reduces charge.' Available at <https://rsf.org/en/news/investigative-reporter-freed-provisionally-after-prosecutor-reduces-charge>; Freedom House (2017) 'Freedom in the World 2017.' Available at <https://freedomhouse.org/country/rwanda/freedom-world/2017>

Access to Information

31. In 2013, the Access to Information Law (**ATI Law**)[60] was enacted. This legislation is supplemented by 5 ministerial orders.[61]

32. While this is a positive development, the lack of appropriate sanctions - in the form of monetary fines with minimum and maximum limits - for information officers who deliberately withhold information requested through the appropriate procedures, inhibits the proper realisation of access to information.

33. Despite the Office of the Ombudsman (**Ombudsman**) possessing powers to impose 'disciplinary sanctions,'[62] this discretionary power does not translate into appropriate sanctions following an officer's failure to disclose information.

34. We note that this failure limits the public's and the media's ability to access information.[63] In line with international best practices, appropriate sanctions need to be provided for the following provisions:

- **Article 9:** Failing to respond within the specified time period to a request for information;
- **Article 12:** Failing to respond to a request to correct personal information; and
- **Article 13:** Failing to respond to requests concerning the exercise of rights and public interest (applicable to private and public bodies), amongst others.

---

60 Law N° 04/2013 of 08/02/2013 Law Relating to Access to Information. Available At <mhc.gov.rw/fileadmin/user_upload/placeholder/Laws_and_Regulations/Itegeko_Rigenga_Kubona_Amakuru.pdf >

61 The ATI ministerial orders include: - N°005/07.01/13 of 19/12/2013: Ministerial Order determining which information could destabilize national security. Available at <ombudsman.gov.rw/en/IMG/pdf/7.d.-_access_to_information__ministerial_order_determining_which_information_could_destabilize_national_security.pdf>; N°006/07.01/13 of 19/12/2013: Ministerial Order determining in details the information to be disclosed. Available at <ombudsman.gov.rw/en/IMG/pdf/7.a.-_access_to_information__ministerial_order_determining_in_details_the_information_to_be_disclosed.pdf>; N°007/07.01/13 of 27/12/2013: Ministerial Order determining the time limit for the provision of information or explanations of not providing it.Available at <ombudsman.gov.rw/en/IMG/pdf/7.c.-_access_to_information__ministerial_order_determining_the_time_limit_for_the_provision_of_information_or_explanations_or_not_providing_it.pdf>; N°008/07.01/13 of 19/12/2013: Ministerial Order determining the procedure of charges of fees related to access to information. Available at <ombudsman.gov.rw/en/IMG/pdf/7.b.-_access_to_information__ministerial_order_determining_the_procedure_of_charges_of_fees_related_to_access_to_information.pdf>; and N°009/07.01/13 of 19/12/2013: Ministerial Order determining private organs to which the Law relating to access to information applies. Available at <ombudsman.gov.rw/en/IMG/pdf/7.e.-_access_to_information__ministerial_order_private_organs_to_which_the_law_relating_to_access_to_information_applies.pdf>

62 Article 10, Law determining the mission, powers, organization and functioning of the Office of the Ombudsman (Law No 76/2013 of 11/9/2013). Available at <http://ombudsman.gov.rw/en/IMG/pdf/office_of_the_ombudsman__law_no_76-2013_office_of_the_ombudsman.pdf>. This provision permits the imposition of "disciplinary sanctions … against any employee whether Government, public or private who acted unjustly towards a person, an organization or an independent association, after written explanations and to determine what should be done so that those who suffered from injustice may find redress."

63 The East African (2016) 'Media, public access to govt information remains 'difficult.' Available at <https://www.theeastafrican.co.ke/rwanda/News/Media-public-access-to-govt-information-remains-difficult/1433218-3401038-nfl6k1z/index.html>

35. The right to access information is further undermined by the National Security Ministerial Order.[64] Worryingly, Article 10 permits the imposition of prior restraint measures where "the level of classified information is doubtful."[65] This provision provides unlimited discretion to authorities, using an indeterminate provision, to judge what information can and cannot be availed to the public.

36. As ARTICLE 19 has noted, this provides persons 'who may have incentives to keep material out of public reach (with the tools to) undermine the right to freedom of information.'[66] Worryingly, this discretion is extended to information officers under Article 13, National Security Ministerial Order. The African Commission on Human and Peoples' Rights, under Principle 26, Model Law on Access to Information in Africa,[67] magnified that information should not be exempted "merely on the basis of its classification status."[68]

37. The Ombudsman is charged with 'monitoring the enforcement' of the ATI Law.[69] In theory and in practice, the Ombudsman's functional and operational independence is not guaranteed. Despite Article 3 of Law No 76/2013[70] magnifying the importance of an independent office, it assumes this independence without providing specifics as to how that independence is ensured. Secondly, the Ombudsman's autonomy is limited given the oversight exercised by the Office of the President.[71] This lack of independence has affected the proper implementation of the ATI Law.

---

64 Ministerial Order determining which information could destabilize national security (N°005/07.01/13 of 19/12/2013). Available at <ombudsman.gov.rw/en/IMG/pdf/7.d._access_to_information__ministerial_order_determining_which_information_could_destabilize_national_security.pdf>

65 Article 10, Ministerial Order determining which information could destabilize national security (N°005/07.01/13 of 19/12/2013) <ombudsman.gov.rw/en/IMG/pdf/7.d._access_to_information__ministerial_order_determining_which_information_could_destabilize_national_security.pdf>

66 ARTICLE 19 (2004) 'Memorandum on the Law On Classified Information of The Former Yugoslav Republic of Macedonia.' Available at <https://www.refworld.org/publisher,ART19,COUNTRYREP,MKD,4756cfbb0,0.html>

67 African Commission on Human and Peoples' Rights 'Model Law on Access to Information in Africa.' Available at <https://www.achpr.org/legalinstruments/detail?id=32>

68 *Ibid*.,

69 Article 17, Access to Information Law (No. 04/2013). Available at <mhc.gov.rw/fileadmin/user_upload/placeholder/Laws_and_Regulations/Itegeko_Rigenga_Kubona_Amakuru.pdf>; Article 4 (15), Law determining the mission, powers, organization and functioning of the Office of the Ombudsman (Law No 76/2013 of 11/9/2013). Available at <http://ombudsman.gov.rw/en/IMG/pdf/office_of_the_ombudsman__law_no_76-2013_office_of_the_ombudsman.pdf>

70 Article 3, Law determining the mission, powers, organization and functioning of the Office of the Ombudsman (Law No 76/2013 of 11/9/2013). Available at <http://ombudsman.gov.rw/en/IMG/pdf/office_of_the_ombudsman__law_no_76-2013_office_of_the_ombudsman.pdf>

71 Annex I, Prime Minister's Order No 51//03 of 27/2/2015 Determining Organisational Structure, Salaries and Fringe Benefits for Employees in the Office of the Ombudsman Official Gazette No. Special Bis of 28/02/2015, pp. 10. Available at <http://ombudsman.gov.rw/en/IMG/pdf/office_of_the_ombudsman__organisational_structure_salaries_and_fringe_benefits_for_employees_of_the_office_of_the_ombudsman.pdf>

38. The Rwanda Civil Society Coalition on UPR (2018), reported that the full realisation of the right to access information is affected by limited awareness of the law by the general public, and "government custodians of information."[72]

39. Some interviewees have commented that some public bodies do not respond to information requests within the stipulated time period. Notably, out of 4 information requests[73] sent to RURA, the Ministry of ICT, the Rwanda Development Board and the Rwanda Information Society Authority, only 1 body responded, by transferring the information request to other government bodies.

40. The interviewees noted that this transfer failed to adhere to the prescribed time limit.[74] Specifically, the body responded to the request after 11 days, rather than the cumulative 6 days, placed the transfer burden on the interviewees instead of transferring the request themselves as prescribed, and further failed to provide the interviewees with the address of the organs to which the application should have been transferred.[75]

41. Thirdly, the interviewees noted that the remaining 3 organs failed to respond to the information requests, contrary to the stipulated 3 day period under Article 2, Ministerial Order - Time Limit. No response has been received as at 9 July 2020.

Recommendations

- Amend the ATI Law and provide for minimum and maximum monetary fines where information officers do not respond to ATI requests.
- Amend the National Security - Ministerial Order and delete vague provisions permitting the restriction of the right to ATI.
- Undertake awareness-raising initiatives to heighten citizens' awareness and government bodies' knowledge of the right to information.
- Guarantee the functional and operational independence of the Office of the Ombudsman and ensure all government departments are consistently and proactively disclosing information and meeting their ATI Law obligations.

---

72 Rwanda Civil Society Coalition on UPR (2018) 'Mid-Term Assessment Report of the Implementation of 2015 UPR Recommendations by the Republic of Rwanda', pp. 11. Available at <https://www.legalaidrwanda.org/spip.php?article132>

73 The interviewees sought information on Rwanda's telecommunications infrastructure.

74 Article 4, Ministerial Order determining the time limit for the provision of information or explanations of not providing it. Available at <ombudsman.gov.rw/en/IMG/pdf/7.c._access_to_information__ministerial_order_determining_the_time_limit_for_the_provision_of_information_or_explanations_or_not_providing_it.pdf>

75 *Ibid.,* Article 4, Ministerial Order (Time Limit) provides that an information officer must transfer the information application to the relevant organ 'no later than 2 days from the date of receipt of an information request.' Article 4 further provides that the information officer shall, no later than 4 days from the date of receipt of the application inform the applicant about the transfer.' Lastly, the information officer is mandated to 'inform the applicant about the transfer and the address of the organ to which the application has been transferred.'

Privacy and Data Protection

ICT Law: Search, Seizure, and Surveillance

42. ARTICLE 19's analysis[76] highlighted a number of search, seizure, and surveillance measures which are subject to abuse, including Articles 33, 123 and 180, ICT Law.[77]

43. Articles 33 and 180, ICT Law provide judicial police officers and RURA powers to search, seize and/or inspect electronic communication systems or equipment, including radio communication. This authority, under Article 33, ICT Law extends to the boarding of 'any vessel, aircraft or vehicle' which amounts to 'limitless jurisdiction without court oversight.'[78] These provisions fail to provide for judicial oversight and rely on 'reasonable grounds', rather than 'probable cause' which is a higher evidentiary threshold.

44. Article 123, ICT Law places a mandatory obligation on intermediaries to "equip the electronic communications network and service with technical instruments and features that allow and facilitate the lawful interception of electronic communications and monitoring." In our view, this is problematic for the following reasons:

- 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; reports in 2015 revealed that the government of Rwanda sought to purchase sophisticated malware and other surveillance tools from an Italian-based hacking firm.

- It mandates the installation of interception tools which compromises users who use encryption tools. The protection of anonymity is a vital component in protecting the rights to freedom of expression and privacy. Further, where anonymity or encryption technologies are in use, providers may be unable to furnish communications to the government. Article 123, ICT Law threatens providers with penalties for failing to cooperate if they are unable to decrypt data or communications. The Special Rapporteur on the Right to Freedom of Opinion and Expression noted that compelled decryption orders - without judicial oversight - restrict expression and privacy and hence are subject to the three-part test under international law.[79]

---

76 ARTICLE 19 (2018) 'Rwanda: 2016 Law Governing Information and Communication Technologies' <https://www.article19.org/resources/rwanda-law-governing-information-and-communication-technologies/>

77 Law Governing ICT, Law No. 24/2016 of 18 June 2016. Available at <http://minict.gov.rw/fileadmin/Documents/Policies_and_Rugulations/ICT_laws/ICT_LAW.pdf>

78 *Ibid*., n. 78.

79 UN Human Rights Council (2013) 'Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to

- It requires operators to install 'backdoors' which allow the circumvention of encryption measures. This not only introduced vulnerabilities into services, but contradicts Article 125, ICT Law which requires operators to keep networks fully secure.[80]

Surveillance

45. We note that the Law on Interception[81] and the ICT Law[82] both raise concerns for the protection of the rights to privacy and freedom of expression.[83]

46. Article 6, Law on Interception grants government authorities of relevant national security organs (including the Rwanda National Police, the Rwanda Defence Force, the National Intelligence and Security Service and the Rwanda Investigation Bureau)[84] authorisation to apply for an interception warrant from a National Prosecutor designated by the Minister.

47. In our view, the Law on Interception fails to comply with international standards on freedom of expression and privacy for the following reasons:

- **Article 3:** permits an arbitrary and vague reliance on 'national security' to justify the exercise of broad surveillance powers in the absence of a requirement that such powers should only be authorised where necessary and proportionate.

- **Article 9:** grants surveillance powers which are not authorised by a court or other independent adjudicatory body but by the national prosecutor who is himself designated by a Minister, i.e., a member of the Executive.

48. The Law on Interception also fails to specify the types of communication subject to interception (*i.e., real time or historic*), to provide the right to notice (*i.e., to be informed of the interception*), or to allow for a claim for damages where the right to privacy has been improperly violated.

---

freedom of opinion and expression' A/HRC/23/40, para 57. Available at <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>

80 *Ibid*., n. 78.

81 Law Regulating the Interception of Communications, Law N°60/2013 of 22/08/2013 . Available at <www.ombudsman.gov.rw/IMG/pdf/24._itegeko_rigena_igenzura_ry_itumanaho_no_60-2013.pdf+&cd=1&hl=en&ct=clnk&gl=ke>

82 Law Governing ICT, Law No. 24/2016 of 18 June 2016. Available at <http://minict.gov.rw/fileadmin/Documents/Policies_and_Rugulations/ICT_laws/ICT_LAW.pdf>

83 The High Commissioner for Human Rights magnified State-level surveillance challenges, including "(in)adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy." United Nations Human Rights - Office of the High Commissioner for Human Rights 'The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights', A/HRC/27/37, para. 47. Available at <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/27/37>

84 In 2018, an amendment to the Criminal Procedure Code proposed to grant the Office of the Ombudsman powers to intercept communications during corruption-related investigations.' See: The New Times (2018) 'How the new law on criminal procedure will boost graft fight.' Available at <https://www.newtimes.co.rw/news/criminal-law-graft-fight>

49. Further, the Law on Interception provides a monitoring framework which is not independent, given the Presidential appointment of inspectors who monitor the legality of officers' interception of communication. Lastly, the Law on Interception fails to provide for independent judicial oversight as well as Parliamentary accountability, given the lack of clarity regarding the authorisation and exercise of surveillance powers (*i.e., number of, and reasons for granting, interception warrants*).

50. The UN Human Rights Committee (2016), in its review of Rwanda's compliance with its obligations under the ICCPR, recommended that interception and use of communications data only "take place on the basis of specific and legitimate objectives and that the categories of circumstances in which such interference may be authorized and the categories of persons likely to be intercepted are set out in detail."[85]

SIM Card Registration

51. In 2018, the government issued the SIM Cards Regulations.[86] These SIM Cards Regulations mandate the collection of biometric (fingerprint) data and the prior production of an 'original ID card' before one receives a SIM card.[87] In 2019, RURA issued a press release restricting network users from having more than 3 SIM cards and subscribers were expected to 'self deregister any extra SIM cards by 31 January 2019.'[88]

52. Mandatory SIM card registration processes heighten governments' ability to monitor and access data of mobile phone users. Instructively, Article 25, SIM Cards Regulations permits RURA to "have access to (an operator's) SIM cards registration database."[89] This provision grants RURA, *whose lack of independence has been enumerated above*, potentially limitless access to users' data. We are concerned that this provision threatens to undermine the confidentiality of digital communications and places restrictions on digital anonymity which is integral to the work of journalists and human rights defenders.

85 Human Rights Committee, Concluding observations on the fourth periodic report of Rwanda, CCPR/C/RWA/CO/4, para. 36. Available at <http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsu6TPkCKzgpozbgBf1JMuskGqdPdoUqXoP88Lh304f6Pg75nbinT6Mrd%2B81fIlBWyxdX%2BDQmDBDvvm0HXtxz4TcOqR2R8B7NaeH1UAvgUPQP>

86 Regulation N ° 004/R/ICT/RURA/2018 Governing the SIM Cards Registration in Rwanda. Available at <https://rura.rw/fileadmin/Documents/ICT/Laws/REGULATION__GOVERNING_THE_SIM_CARDS_REGISTRATION_IN_RWANDA.pdf>

87 *Ibid.,* Article 7.

88 RURA (2019) 'Press Release - SIM Cards Limitation.' Available at <197.243.22.137/rura7/fileadmin/publication/SIM_Card_Limitation.pdf>

89 Article 25. *Ibid*., n. 89.

53. In 2018, Citizen Lab revealed that the Rwandan government was using Pegasus, an NSO Group (Israel) surveillance software to monitor journalists, activists and opposition members.[90] Pegasus allegedly permitted the remote installation of malware designed 'to intercept and extract information and communications from mobile phones and devices… and enable the remote access and control of information including calls, messages, and location—on mobile devices using the Android, iOS, and BlackBerry operating systems.'[91]

Digital Identity System

54. Since 2014, Rwanda has been working on establishing a national digital ID program. In 2016, Rwanda announced its proposed establishment of electronic ID (or **eID)** for online and offline identification.[92] In 2017, Rwanda established the Irembo eGovernment Portal,[93] which includes the eID program. Crucially, digital identity systems which are backed by the state's powers and resources, must be designed and implemented using sound governance, data protection, privacy and security principles. Further, comprehensive policy and legislative frameworks are a necessary prerequisite, given the data heavy nature of these programs at the enrollment, storage, and use stages, especially where biometric and DNA data is being collected.

55. Access Now's policy paper[94] documented various risks associated with centralised and government-managed digital identity systems. The mandatory use and collection of biometric data in the new digital ID cards in Rwanda raises unique concerns, including:

- Unchecked and mass surveillance initiatives and the exacerbation of discrimination and exclusion against vulnerable communities and target groups,[95] given the sensitivity and the particularities of biometric data;

- Additional identity risks faced by individuals' - especially with biometric data - of malicious hacking and cyber intrusion by private actors, including criminals, especially where digital ID programs are not supported by an equally strong technology and cybersecurity environment.

56. Notably, the aggregation and use of biometric data should be sharply limited, even if such aggregation and use is aimed at increasing convenience or justified as a way to enhance security.

---

90 Freedom House (2019), 'Freedom on the net - Rwanda'. Available at <https://freedomhouse.org/country/rwanda/freedom-net/2019>

91 Marczak B, Scott-Railton S, McKune S, Razzak B A, and Deibert R (2018) 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries.' Available at <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>

92 Biometric Update.Com (2016) 'Rwanda to introduce new eID card'. Available at <https://www.biometricupdate.com/201605/rwanda-to-introduce-new-eid-card>

93 Irembo eGovernment Portal. Available at <https://irembo.gov.rw/rolportal/en/web/nida/application-for-national-id>

94 Access Now (2018) 'National Digital Identity Programmes: What's Next?' Available at <https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf>

95 Access Now (2018) 'National Digital Identity Programmes: What's Next?' Available at <https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf>

57. Despite President Kagame previously issuing positive statements recognising the role of trust,[96] the need for information to be 'protected from unauthorised access as well as clarity on the ownership and management of people's personal data,'[97] they do not reflect the reality of the government's use of technology (*as identified above*).

58. Access Now and ARTICLE 19 note that "trust" in digital ID programs is not only a matter of implementing appropriate data governance systems or formally providing safeguards to protect individuals' rights. It is also a matter of ensuring that the data processed within a digital ID program does not serve illegitimate governmental interests, by threatening, harming and undermining critical voices.

Informational Privacy (or Data Protection)

59. The right to privacy and the protection of personal information is protected under Articles 23 and 38 of the Constitution.[98] Commendably, Rwanda ratified the Malabo Convention in 2019.[99] In accordance with Article 168 of the Constitution, the Malabo Convention was incorporated into Rwanda's national law following a presidential order.[100] However, Rwanda continues to operate without a functional and independent data protection authority.

Recommendations

- Amend Articles 33, 123 and 180 of the ICT Law to align them with international standards on freedom of expression and privacy.
- Revise the Law of Interception (2013) to align it with international standards on freedom of expression and privacy.
- Revise the SIM Card Regulations to align it with international standards on freedom of expression and privacy, especially Article 25, SIM Card Regulations which threatens to undermine digital anonymity.
- Ensure that the digital identification programme does not integrate unlawful surveillance and repressing practices against journalists, activists and opposition members.
- Minimise the amount and type of data collected by the government and associated service providers through the digital identification system and ensure that enrollment

96 President Kagame maintained that "digital systems can only function well when they are trusted." The New Times (2019) 'Kagame makes case for African digital identity'. Available at <https://www.newtimes.co.rw/news/kagame-african-digital-identity>

97 The New Times (2019) 'Kagame makes case for African digital identity'. Available at <https://www.newtimes.co.rw/news/kagame-african-digital-identity>

98 Before the Malabo Convention was ratified, various sectoral laws inadequately catered for the right to informational privacy, including Article 4(3), ATI Law, Chapter VIII, Penal Code, Articles 102 and 124, ICT Law (2016) and Article 27, SIM Cards Regulations. The draft 'Regulations Governing the Use of Personal Data in Rwanda' - which were prepared by RURA in 2019 - were not adopted.

99 The African Union Convention on Cyber Security and Personal Data Protection, 27 June, 2014 (EX.CL/846 (XXV)). Available at <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

100 Presidential Order No 104/01 of 18/09/2019 Ratifying the African Union Convention on Cyber Security and Personal Data Protection Adopted in Malabo, Equatorial Guinea on 27 June 2014. Available at <https://www.minict.gov.rw/index.php?id=102>

or participation in the identity program is not a prerequisite to receive essential goods and services.

- Restrict unlawful interception and monitoring of digital identity use and implement measures for accountability.
- Operationalise an independent data protection authority and ensure the full implementation of the Malabo Convention.

Internet Access

60. Rwanda accepted 1 recommendation aimed at advancing digital rights, by continuing to grant access to the Internet to its population, especially underprivileged communities.[101]

61. Commendably, the government has taken steps to improve Internet access[102] as part of Rwanda's Vision 2020[103] and its Smart Rwanda Master Plan.[104] Rwanda's Universal Access Fund (the **UAF**) is provided in Article 18, ICT Law and given further effect in Presidential Order (Fund) 2004.[105] The UAF is described as intended to create an 'enabling environment for people to have equal opportunity and access to telecommunications services' in a timely and affordable manner.'[106]

62. RURA's 2018 – 2019 Annual Report[107] notes that UAF funds - Frw 2.7 billion (2,812,090 USD) - were used to finance various initiatives. These included the installation of Internet in '193 schools located in rural and underserved areas and the construction and operationalisation of 10 telecommunication sites.'[108]

---

101 133.34. *Continue with the impressive process of granting access to the Internet to its population, in particular to underprivileged communities* (Haiti).

102 Notably, the government has invested heavily in Rwanda's internet infrastructure and other ICTs, including the laying of over 4, 500Km+ national fibre optic broadband cabling and the deployment of a 'single wholesale 4G broadband network'. See: Rwanda Development Board 'Overview.' Available at <https://rdb.rw/investment-opportunities/ict/> ; UN-OHRLLS (2017) 'Leveraging Investments in Broadband for National Development; The Case of Rwanda and Senegal.' Available at <http://unohrlls.org/leveraging-investments-in-broadband-for-national-development-the-case-of-rwanda-and-senegal>

103 Rwanda's ambitious Vision 2020 (2012 – 2020) set out to provide "internet access at all administrative levels, for all secondary schools and for a large number of primary schools." It also anticipated a '60% rise in mobile subscriptions internet penetration rates (users) to at least 50%.' See: Republic of Rwanda 'Rwanda Vision 2020 (revised 2012)' pp. 14. Available at <https://www.greengrowthknowledge.org/national-documents/rwanda-vision-2020-revised-2012>

104 This "constitutes part of the fourth generation national information and communications infrastructure (or **NICI**) plans" aimed at transforming the country into a knowledge-based society. See: Republic of Rwanda Ministry of Youth and ICT (2016) 'Smart Rwanda Master Plan', pp. 6. Available at <https://minict.gov.rw/index.php?id=54&tx_kesearch_pi1%5Bsword%5D=Smart+Rwanda+Master+Plan&tx_kesearch_pi1%5Bpage%5D=1&tx_kesearch_pi1%5BresetFilters%5D=0&tx_kesearch_pi1%5BsortByField%5D=&tx_kesearch_pi1%5BsortByDir%5D=>

105 Presidential Order No ° 05/01 of 15/03/2004 Determining the Functioning of the Universal Access Fund and Public Operator's Contributions. Available at <https://www.rura.rw/index.php?id=104&tx_news_pi1%5Bnews%5D=35&tx_news_pi1%5Bday%5D=26&tx_news_pi1%5Bmonth%5D=4&tx_news_pi1%5Byear%5D=2017&cHash=7e8d6227c84ac18c6fcc808577a18aea>

106 Article 3(3), Law Governing ICT, Law No. 24/2016 of 18 June 2016. Available at <http://minict.gov.rw/fileadmin/Documents/Policies_and_Rugulations/ICT_laws/ICT_LAW.pdf>

107 RURA 'Annual Report 2018 – 2019.' Available at <https://rura.rw/index.php?id=29>

108 *Ibid*., pp. 38 - 39.

63. It is not possible to analyse the extent to which RURA has fulfilled the UAF's objectives to enhance access for marginalised and underprivileged groups. This stems from a persistent reporting failure by RURA, to provide the total UAF budget against the amount spent by the UAF *per annum* for specific projects. Secondly, there is a lack of clarity in the report about the specific schools and areas which benefited from UAF funds.

64. These failures contravene Article 3 (8), Ministerial Order (Information Disclosure)[109] which requires public bodies to proactively disclose information related to the "budget allocated to each department of the organ, indicating the planning and reports on disbursements made."[110] In this regard, a greater commitment to proactive disclosure is needed, in accordance with international standards on access to connectivity information held by RURA.

65. Despite commendable Rwanda's efforts to expand Internet access to its population, uptake has been extremely slow. The International Telecommunication Union reports that only 9.7 million[111] people had access to a mobile phone in 2018, despite this being the primary means of connecting to the Internet and a growing population rate (12.5 million people in 2018).[112] On the other hand, the World Bank reports an internet penetration rate of 21.768% (2017) from 20% (2016).[113]

66. Further, Research ICT Africa notes that the rural-urban digital divide in Rwanda has not been narrowed, as evidenced by the continued concentration of Internet use in the urban area, Kigali, with a "very small portion of the population residing in rural areas using the Internet."[114]

Recommendations

- Fully protect the right to freedom of expression and information online by taking proactive steps to improve access to the Internet.
- Publish annual transparency reports providing comprehensive details about the amount of money collected under the Universal Access Fund per annum, and the amount spent on implemented projects in line with international reporting standards.

---

109 Ministerial Order determining in details the information to be disclosed (N°006/07/01/13 of 19/12/2013). Available at <ombudsman.gov.rw/en/IMG/pdf/7.a._access_to_information__ministerial_order_determining_in_details_the_information_to_be_disclosed.pdf>

110 *Ibid.,*

111 ITU 'Country ICT Data: Mobile-Cellular Subscriptions.' Available at <https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Mobile_cellular_2000-2018_Dec2019.xls>

112 World Bank (2019) 'The World Bank in Rwanda: Overview.' Available at <https://www.worldbank.org/en/country/rwanda/overview>

113 World Bank 'Individuals using the Internet (% of population) – Rwanda.' Available at <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=RW>

114 Gillwald, A & Mothobi, O (2019) '*After Access 2018: A demand-side view of mobile Internet from 10 African countries*', pp. 17. Available at <https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf>