

May 27,

2020

Joint Letters

Re: Use of cybercrimes
legislation to restrict
fundamental rights and
freedoms in Kenya and
Nigeria

Mr. David Kaye

United Nations Special
Rapporteur on the
Promotion and Protection of
the Right to Freedom of
Opinion and Expression

4 0 1 East Peltason D r i v e
3 8 0 0 -C
Irvi n e, CA 92697 - 8 0 0 0
(9 4 9) 824-2427

Signatories:

Amnesty International

ARTICLE 19 Eastern Africa

BudgIT

Centre for Intellectual Property

and Information Technology Law

(CIPIT), The

Co Creation Hub (CcHub)

Collaboration on International

ICT Policy for East and Southern

Africa (CIPESA), The

Kenya ICT Action Network

(KICTANet)

Legal Resource Centre (LRC)

Paradigm Initiative (PIN)

Re: Use of cybercrimes
legislation to restrict
fundamental rights and
freedoms in Kenya

May 27, 2020

We, the undersigned nine (9) civil society organisations (or partner organisations), coming together as African Internet Rights Alliance (AIRA) write to express our deep concern about Kenya's Computer Misuse and Cybercrimes Act (or CMCA, 2018) - or "fake news" - law.

We call on your Excellency to take note and advise against this framework as it is a threat to the protection and promotion of freedom of expression, access to public health information, media freedom, and privacy. In particular, CMCA, 2018 envisages a nation with only one truth and creates ambiguous offences criminalising 'fake news.' It also sets unjustifiable barriers to legitimate expression by making it illegal to send even a single 'communication that is likely to cause apprehension.' This is a threat to legitimate expression that already has a chilling effect on civic space and digital rights in the country.

We would therefore like to draw Your Excellency's attention to the potential and actual threats posed by the CMCA, 2018, which directly contravenes Kenya's regional and international human rights law obligations and commitments. Notably, the CMCA, 2018 provisions are having a demonstrable impact on the right to free expression and privacy, and fail to comply with Kenya's obligations under Article 9, African Charter on Human and Peoples' Rights (or African Charter) and Article 19, the International Covenant on Civil and Political Rights (or Covenant).

The situation in Kenya is dire, and the ability of Internet users to freely express themselves online in an open and protected manner, is being systematically undermined by the government. This has particularly worsened during the COVID-19 pandemic, where freedoms, particularly movement, access to courts, as well as economic and social rights are being curtailed by the government's possession of extraordinary powers. The government, claiming to be the only source of truth, has threatened and arrested people for raising governance issues on the management of the pandemic.

The partner organisations recognise the need to combat economic crimes committed using digital technologies, as well as the need to curb misinformation and other Internet-related challenges during this public health pandemic. However, this framework has created a powerful instrument enabling authorities to arbitrarily monitor and regulate the activities of Internet users and control free expression online, in the absence of adequate safeguards.

Background - Judicial Petition

In 2018, the Bloggers Association of Kenya, ARTICLE 19 Eastern Africa and the Kenya Union of Journalists contested the legality and constitutionality of the CMCA, 2018. The Petitioners challenged twenty-six (26) provisions - including sections 22, 23 and 27, CMCA, 2018 - in the *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)*. [2020] eKLR.

Despite the High Court of Kenya upholding the constitutionality of the CMCA, 2018 in its entirety on 20 February 2020, various provisions continue to impose chilling restrictions on the right to freedom of expression, privacy, and press freedom. This decision is currently being appealed at the Court of Appeal level.

Problematic Provisions

1. 'Misinformation' and COVID-19: Kenya

The partner organisations have monitored instances where broad and vague 'misinformation' provisions - under sections 22 and 23, CMCA, 2018 - have been used to intimidate, arrest, detain and charge Internet users. These two (2) provisions have been turned into overt surveillance tools which are being used to intimidate Internet users with offline and online effects, including the forced removal of content and the exercise of self-censorship to evade sanctions.

Section 22, CMCA, 2018 provides as follows:-

1. *"A person who intentionally publishes false, misleading or fictitious data or misinforms with intent that the data shall be considered or acted upon as authentic, with or without any financial gain, commits an offence and shall, on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.*

2. *Pursuant to Article 24 of the Constitution, the freedom of expression under Article 33 of the Constitution shall be limited in respect of the intentional publication of false, misleading or fictitious data or misinformation that—*

- (a) *is likely to —*
 - i. *propagate war; or*
 - ii. *incite persons to violence;*
- (b) *constitutes hate speech;*
- (c) *advocates hatred that —*
 - i. *constitutes ethnic incitement, vilification of others or incitement to cause harm; or*
 - ii. *is based on any ground of discrimination specified or contemplated in Article 27(4) of the Constitution; or*
- (d) *negatively affects the rights or reputations of others."*

On the other hand, 23, CMCA (2018) provides as follows: *"A person who knowingly publishes information that is false in print, broadcast, data or over a computer system, that is calculated or results in panic, chaos, or violence among citizens of the Republic, or which is likely to discredit the reputation of a person commits an offence and shall on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding ten years, or to both."*

At the time of writing, four (4) persons have been summoned by the Directorate of Criminal Investigations (or DCI) for allegedly publishing ‘false COVID-19 information which is calculated or results in panic’ in March 2020 alone. Out of these four (4) individuals, two (2) bloggers have been charged under section 23, CMCA, 2018 and their matters are currently ongoing.

The partner organisations note that section 23, CMCA, 2018 is broad and vaguely-worded and has imposed a legal duty of ‘truth’ in Kenya. In turn, this legal duty fails to respect the maxim that ‘protections under the right to freedom of expression are not limited to truthful statements and information.’ Additionally, these ‘misinformation’ provisions carry steep sanctions and impose custodial sentences which raise concerns about their necessity and proportionality.

Lastly, the partner organisations are greatly concerned that the High Court, in upholding section 23, CMCA, 2018 re-introduced criminal defamation in Kenya. This was previously declared unconstitutional in *Jacqueline Okuta & another v Attorney General & 2 others* [2017] eKLR.

Your Excellency, the High Court in *Jacqueline Okuta* correctly noted that resorting to criminal, rather than civil remedies following an injury to a person's reputation is “unnecessary, disproportionate and therefore excessive and not reasonably justifiable in an open democratic society based on human dignity, equality and freedom.”

Your Excellency has often reiterated the incompatibility of criminal defamation provisions with the right to freedom of expression in various statements, the Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propoganda and the Joint Declaration on Media Independence and Diversity in the Digital Age that “*states are under a positive obligation to create a general enabling environment for seeking, receiving and imparting information and ideas (freedom of expression), including... ensuring that defamation laws are exclusively civil rather than criminal in nature and do not provide for excessive damages awards.*”

The partner organisations have also noted ongoing efforts by senior government officials to reinforce this environment of intimidation by issuing ‘warning’ statements on print and broadcast media. Instructively, the Cabinet Secretary for Health in Kenya maintained the following:

"these rumours must stop ... but because I know empty appeals will not work, we will proceed and arrest a number of them to prove our point."

These statements are supported by the public circulation of government-sanctioned statements on social media platforms highlighting any action taken to censure ‘offending’ Internet users.

2. Cyber Harassment Provision: Kenya

In Kenya, the cyber harassment provision under section 27, CMCA, 2018 has granted the Kenyan government - including the DCI - power to prosecute people for voicing their concerns or speaking truth directly to individuals. Section 27, CMCA, 2018 provides as follows:-

1. *"A person who, individually or with other persons, wilfully communicates, either directly or indirectly, with another person or anyone known to that person, commits an offence, if they know or ought to know that their conduct—*

- a. is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property; or*
- b. detrimentally affects that person; or*
- c. is in whole or part, of an indecent or grossly offensive nature and affects the person."*

At the time of writing, the partner organisations note the potential threat this provision poses to the rights of free expression and privacy. This cyber-harassment provision is vaguely worded and has the potential to lead to convictions for single and one-off, rather than repeated, communication(s). This provision carries a penalty, upon conviction, of a KES. twenty (20) million (c. \$184, 520) fine or a ten (10) year imprisonment period.

Rule of Law in Kenya

The utilisation of punitive civil and criminal sanctions and custodial sentences in the CMCA, 2018 continues to entrench an environment of fear and censorship. This is taking place in the context of a global pandemic which has crippled the efficacy of judicial services across Kenya.

The independence of the Kenyan judiciary and its effective dispensation of justice is also under threat, given heightened governmental pressure. On a scale of 1-7 (7 being ‘entirely independent’), the World Economic Forum puts the Kenyan judiciary at 4.2.

Instructively, the Chief Justice of Kenya issued a pre-COVID 19 statement in 2019 which revealed the extent of judiciary budgetary cuts which were sanctioned by the Executive and Parliament. These cuts led to the suspension of judicial services, including the operation of mobile courts and tribunals, and the deployment of judicial developments, including its ICT programme and internet services to courts in Kenya.

Based on the foregoing, it is clear that constitutional petitions to protect threatened rights and freedoms - including freedom of expression, privacy and media freedom - were also greatly affected by these cuts. Crucially, these cuts were successfully contested by the Law Society of Kenya in 2019.

Additionally, in early 2020, the President issued a stern warning to the judiciary to refrain from ‘slowing down government projects.’

In line with your mandate to “make recommendations and provide suggestions on ways and means to better promote and protect the right to freedom of opinion and expression in all its manifestations,” we strongly urge your Excellency to call on the government of Kenya to:

1. Place a moratorium on the use of its CMCA, 2018 framework, and the ‘fake news’ and cyber-harassment provisions specifically;
2. Drop all misinformation charges imposed on any individuals using the CMCA, 2018, or any other related legislative frameworks;
3. Review any current civil and/or criminal cases where persons have been fined and/or imprisoned using the provisions in the CMCA, 2018; and
4. Initiate participatory and transparent processes to reform the CMCA, 2018 and ensure its strict compliance with international and regional standards relating to freedom of expression, privacy and media freedom.

We thank you for your attention to these issues, and we offer our assistance and support to protect these rights and the well-being of all those within the territory of Kenya.

Mr. David Kaye

**United Nations Special
Rapporteur on the
Promotion and Protection of
the Right to Freedom of
Opinion and Expression**

4 0 1 East Peltason D r i v e
3 8 0 0 -C
Irvi n e, CA 92697 - 8 0 0 0
(9 4 9) 824-2427

Signatories:

Amnesty International

ARTICLE 19 Eastern Africa

BudgIT

Centre for Intellectual Property

and Information Technology Law

(CIPIT), The

Co Creation Hub (CcHub)

Collaboration on International

ICT Policy for East and Southern

Africa (CIPESA), The

Kenya ICT Action Network

(KICTANet)

Legal Resource Centre (LRC)

Paradigm Initiative (PIN)

**Re: Use of cybercrimes
legislation to restrict
fundamental rights and
freedoms in Nigeria**

May 27, 2020

We, the undersigned nine (9) civil society organisations (or partner organisations), coming together as African Internet Rights Alliance (AIRA) write to express our deep concern about Kenya's Computer Misuse and Cybercrimes Act (or CMCA, 2018) - or "fake news" - law.

We call on your Excellency to take note and advise against this framework as it is a threat to the protection and promotion of freedom of expression, access to public health information, media freedom, and privacy. In particular, CMCA, 2018 envisages a nation with only one truth and creates ambiguous offences criminalising 'fake news.' It also sets unjustifiable barriers to legitimate expression by making it illegal to send even a single 'communication that is likely to cause apprehension.' This is a threat to legitimate expression that already has a chilling effect on civic space and digital rights in the country.

We would therefore like to draw Your Excellency's attention to the potential and actual threats posed by the CA, 2015, which directly contravenes Nigeria's regional and international human rights law obligations and commitments. The partner organisations are concerned that the CA's, 2015 provisions are having a demonstrable impact on various rights, and fail to comply with Nigeria's obligations under Article 9, African Charter on Human and Peoples' Rights (or African Charter) and Article 19, the International Covenant on Civil and Political Rights (or Covenant).

The situation in Nigeria is dire, and the ability of Internet users to freely express themselves online in an open and protected manner, is being systematically undermined by the government. This has particularly worsened during the COVID-19 pandemic, where freedoms, particularly movement, access to courts, as well as economic and social rights are being curtailed by the government's possession of extraordinary powers. The government, claiming to be the only source of truth, has threatened and arrested people for raising governance issues on the management of the pandemic.

The partner organisations recognise the need to combat economic crimes committed using digital technologies, as well as the need to curb misinformation and other Internet-related challenges during this public health pandemic. However, this framework has created a powerful instrument enabling authorities to arbitrarily monitor and regulate the activities of Internet users and control free expression online, in the absence of adequate safeguards.

Background - Judicial Petition

In 2016, Paradigm Initiative, the EiE Project and Media Rights Agenda contested the legality and constitutionality of Nigeria's Cybercrimes (Prohibition, Prevention, etc) Act, (or CA, 2015) framework for being arbitrarily restrictive. The Petitioners challenged two provisions, namely sections 24 and 38, CA, 2015 in *The Incorporated Trustees of Paradigm Initiative for Information Technology Development & 2 Others - vs- the Attorney General of the Federation & 2 Others.*

The High Court and Court of Appeal upheld the problematic and unconstitutional provisions being challenged, and failed to carefully consider the reasoning in the foreign decisions relied on by the Petitioners.

In a concurring judgment, one of the justices, however, agreed that the law should be reviewed to whittle-down its arbitrariness.

Noble as that observation was, it has not proven sufficient to dissuade law enforcement operatives and government officials from continuing to impose these chilling restrictions on the fundamental rights to freedom of expression and privacy (telegraphic conversations and telegraphic communications) and press freedom. The Court of Appeal decision is currently being appealed at the Supreme Court level.

Problematic Provisions

1. Cyber Harassment Provisions: Nigeria

In Nigeria, the ‘cyber-stalking’ provision under section 24, CA, 2015 has granted the Nigerian government power to prosecute people for voicing their concerns, dissent or speaking truth directly to individuals.

This cyber-stalking provision is vaguely worded and has served as the basis for arrests, illegal detentions and convictions for ordinary citizens and journalists who, in the opinion of the government, make communications that cause inconvenience, annoyance, needless anxiety, and even insult.

Healthy public discourse and information sharing about governmental activities and actions have become strained by this law. Instructively, a journalist was arrested for criticising the actions and policies of a State Governor on social media in August 2016. This is just one out of hundreds of Nigerians subjected to this repressive law. Depending on the perceived severity of the threat, this provision carries a N7, 000, 000 - N25, 000, 000 (\$17,871.7 - \$63,827.6) fine and/or a three (3) - ten (10) year imprisonment period.

2. Records Retention and Protection of Data: Nigeria

In Nigeria, a service provider is mandated to keep all traffic data and subscriber information for a period of two (2) years, under the ‘records-retention’ provision (section 38, CA, 2015).

The CA, 2015 also mandates that service providers will release any such information, at the request of relevant authority and law enforcement agencies. This provision is problematic because ‘relevant authority’ is neither defined nor described and the request for private communication data is not subject to judicial review.

Rule of Law in Nigeria

The utilisation of punitive criminal sanctions and custodial sentences in the CA, 2015 continues to entrench an environment of fear and censorship. This is taking place in the context of a global pandemic which has crippled the efficacy of judicial services across Nigeria.

The independence of the judiciary in Nigeria is also under threat, given heightened governmental pressure on the judiciary. On a scale of 1-7 (7 being 'entirely independent'), the World Economic Forum puts the Nigerian judiciary at 3.6.

Further, the pace at which these constitutional petitions have been considered by the Judiciary in Nigeria is a source of great concern. Instructively, the Nigerian Supreme Court received the Applicants' appeal on 29 January 2019. No further communication was received by the Applicants by September 2019, which prompted them to serve letters to the Chief Justice of Nigeria requesting for a hearing date.

As at the writing of this letter in May 2020, the Applicants have still not received any decision on their application for a hearing date.

In line with your mandate to "make recommendations and provide suggestions on ways and means to better promote and protect the right to freedom of opinion and expression in all its manifestations," we strongly urge your Excellency to call on the government of Nigeria to:

1. Place a moratorium on the use of its CA, 2015 framework, and its cyber-harassment and records-retention provisions specifically;
2. Drop all cyber-harassment charges imposed on any individuals using the CA, 2015, or any other related legislative frameworks;
3. Review any current civil and/or criminal cases where persons have been fined and/or imprisoned using the provisions in the CA, 2015; and
4. Initiate participatory and transparent processes to reform the CA, 2015 and ensure its strict compliance with regional and international standards relating to freedom of expression, privacy and media freedom.

We thank you for your attention to these issues, and we offer our assistance and support to protect these rights and the well-being of all those within the territory of Nigeria.

