EXECUTIVE SUMMARY - KENYA

***/The intersection of the right to freedom of expression and protection of personal information.**

This report examines the intersection of the right to freedom of expression online and protection of personal information in Kenya. In doing this, the report is divided into four broad sections. The first section considers the right to freedom of expression, particularly online, by considering various laws, policies and incidents that have either promoted or violated the right in Kenya. The second section of the report examines the status of protection of personal information in Kenya. The third section considers the intersections of both right and the final part concludes.

As the report shows, despite Kenya's various obligations under international human rights standards and the provisions of Article 33 of the 2010 Constitution to protect the right to freedom of expression, the right has suffered a number of setbacks as a result of problematic laws and State-sponsored violations. For example, in defining hate speech which is a legally permissible limitation on the right to freedom of expression, Section 13 of the *National Cohesion and Integration Commission (NCIC) Act* went overboard to include 'insults' in its definition.

Likewise, with respect to online speech, sections 22 and 23 of the *Computer Misuse and Cybercrimes Act* provide for criminal offences for intentional publication of false data, 'fake news' and disinformation which are clear violations of the 2010 Constitution and international human rights law. In addition to this, leaving the award of pecuniary damages to the discretion of judges under Section 16A of *Defamation Act* and failure to assess a defendant's financial capacity could instil a chilling effect on the right to freely express in Kenya.

In addition to these laws, Section 84d of the *Kenya Information and Communications Act*, (KICA) 1998 which has since been declared unconstitutional in 2019 by the High Court in *Cyprian Andama v Director of Public Prosecution & another* criminalised a material that could 'deprave and corrupt persons.' This is largely at odds with the international human rights standards on protecting the right to freely express one's self.

More concerning, is the provision of the *Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Content via Electronic Communications Networks* of 2017 which was released by the Communications Authority of Kenya (CAK). It provides that platforms should take down accounts that disseminate 'undesirable political content' which have been brought to their attention within 24 hours. This provision does not include any form of judicial review or oversight, again, granting the State overboard powers overregulating online speech in Kenya.

However, while these laws and a number of others examined in the full report document the challenges faced by the right to freedom of expression both offline and online within the Kenyan context, the courts seem to have risen to the occasion in many cases. Some of these cases include *Jacqueline Okuta & another v Attorney General & 2 others [2017]* eKL*R* relating to an alleged defamatory Facebook post where the High Court of Kenya ruled that the provisions of Section 194 of the Penal Code on criminal defamation are unjustifiable in a modern society like Kenya. In another case of *Robert Alai v The Attorney General & another* [2017] eKLR, the Court noted that oppressive laws that hide under protecting the dignity of public officers can no longer be used to violate people's right to freedom of expression.

Despite the challenges posed by these problematic laws and governments' illegal actions, in 2019, a proposed amendment to KICA to demand licensing of social media platforms, sharing of information of licensed persons, registration of bloggers and other provisions that pose threats to the right to freedom of expression was rejected by the National Assembly's Departmental Committee on Communication, Information and Innovation. This and many more show that while the mill of protection of the right to freedom of expression grinds slowly, there are strong pushbacks mostly from civil society and the courts.

On the third section on the protection of personal information, Section 31 of the 2010 Constitution guarantees the right to privacy. This is in addition to the various obligations Kenya has to protect the right under international human rights law. In fulfilling these obligations, on 8 November 2019, Kenya's Data Protection Act – the primary and substantive law on data protection became operational. While the law has various challenges including issues relating to its take-off and implementation, it has provided an opportunity to press harder on the need to protect privacy in the digital age in Kenya.

It is also important to note that the law has not come to solve all of Kenya's challenges with respect to protection of personal information. For example, while Kenya's digital ID system, the National Integrated Identity Management System (NIIMS) collects a large trove of sensitive personal information like fingerprints, voice waves, iris patterns etc., there are no clear indications as to how such information will be protected. This has led to the High Court order in January 2020 that the government of Kenya should enact an appropriate and comprehensive regulatory framework that complies with the 2010 Constitution. These show that the right to privacy, and by extension the protection of

personal information in Kenya requires urgent interventions through rights-respecting laws and policies.

The analyses of both rights in Kenya further point to three main intersections namely journalistic exemptions, the right to rectification and erasure and encryption and anonymity further guarantees the protection of rights. In Kenya, the report finds that there is need to expand on the provisions of section 30(b) of the DPA that grants processing of data for journalistic purposes. Additionally, the provisions of section 25(f) of the DPA on erasure and rectification of personal data needs to be operationalised by the Data Protection Regulations 2021 which is yet to come into force while paying to internationally set standards. With respect to encryption, section 41(4) of the DPA requires data processors to secure personal data including the encryption of data while section 37 of the same Act requires that data processing for commercial purposes are anonymised and are made unidentifiable. All of these points to the need to not only protect both the right to freedom of expression and personal information as standalone rights, but also as intersecting rights. This is because they give rise to new concerns for human rights protection that must be looked into which include journalistic exceptions, right to erasure and rectification and encryption and anonymity.