Sudan: Cybercrime Law can restrict vital information during the pandemic

ARTICLE 19 calls on the Sudan Government to immediately repeal its 2018 Cybercrime Law that imposes unacceptable restrictions on the right to freedom of expression. Instead of bringing the Law in compliance with international freedom of expression standards, the amendments, adopted in the summer of 2020, by the joint civilian and military transitional Government introduced even harsher sanctions that can be used to restrict critical voices in the country. Sudanese journalists have been already facing numerous restrictions, including for their reporting on the COVID-19 pandemic, often being branded as "fake news." Harsher penalties provided for in the Cybercrime Law will further silence independent reporting, rather than fighting disinformation.

Background to the Cybercrime Law

In July 2020 the Prime Minister of Sudan Abdalla Hamdok signed amendments to the Law to Combat Information Crimes – the Cybercrime Law of 2018 (the Cybercrime Law) that introduced criminal penalties targeting the spread of 'fake news' online.

It is difficult to ascertain the origin of the Cybercrime Law as it was drafted and passed in 2018 before the Sudan revolution. The certification clause of the Law shows that it was passed by the National Assembly under former President Omar Al Bashir in November 2018, just days before protests broke out all over the country commencing the 2018 revolution. However, since its enactment, the Government of Sudan through the Ministry of Justice has never published or made the Law available to the public in its official gazette which is against the rule of law principles. The only copy of the Law in public circulation was leaked and anonymously uploaded on Google drive. Thus, the Law was enforced without being published, in contrast with the rule of law principles.

In July 2020, the joint civilian and military transitional Government enacted the amendments to the Law which increased sanctions provided for in the 2018 Law. This was followed by an official announcement by the Sudan army confirming that they had appointed a Special Commissioner in May 2020 to take legal action under various laws, including the amended Cybercrime Law, against anyone; including activists and the media, in or outside Sudan, who insult or defame the military online.

In this briefing, ARTICLE 19 highlights the most problematic provisions of the Cybercrime Law and shows how it fails to comply with international freedom of expression standards.

Applicable international freedom of expression standards

The right to freedom of expression is protected by several international human rights instruments, in particular Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR). The African Charter on Human and Peoples' Rights also guarantees freedom of expression in Article 9, and Additional guarantees to freedom of expression are provided in the 2002 Declaration of Principles on Freedom of Expression in

Africa (African Declaration).

Restrictions on the right to freedom of expression must be strictly and narrowly tailored and satisfy a tri-partite test. Specifically, restrictions must:

- **Be prescribed by law**: This means that a norm must be formulated with sufficient precision to enable an individual to regulate their conduct accordingly;

- **Pursue a legitimate aim:** This exhaustively includes respect of the rights or reputations of others, protection of national security, public order, public health or morals;

- **Be necessary and proportionate**: Necessity requires that there must be a pressing social need for the restriction. Proportionality requires that a restriction is specific and individual to attaining that protective outcome and is no more intrusive than its alternatives.

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

It is also important to note that Article 20(2) ICCPR provides that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited by law. At the same time, inciting violence is more than just expressing views that people disapprove of or find offensive. It is speech that encourages or solicits other people to engage in violence through vehemently discriminatory rhetoric. At the international level, the UN has developed the Rabat Plan of Action, an inter-regional multi-stakeholder process involving UN human rights bodies, NGOs and academia – which provides the closest definition of what constitutes incitement law under Article 20 (2) ICCPR.

Although there is no international standard on cybercrime, from a comparative perspective, the 2001 Council of Europe Convention on Cybercrime (the Cybercrime Convention) has been the most relevant standard. Although Sudan is not a signatory to the Convention, it provides a helpful model for States seeking to develop cybercrime legislation.

The Cybercrime Convention provides definitions for relevant terms, including definitions for computer data, computer systems, traffic data and service providers. It requires State parties to create offences against the confidentiality, integrity and availability of computer systems and computer data; computer-related offences including forgery and fraud; and content-related offences such as the criminalisation of child pornography. The Cybercrime Convention then sets out several procedural requirements for the investigation and prosecution of cybercrimes, including preservation orders, production orders and the search and seizure of computer data. Finally, and importantly, the Cybercrime Convention makes clear that the above measures must respect the conditions and safeguards for the protection of human rights and liberties, consistent with the ICCPR and other applicable international human rights instruments.

The Sudanese Government must ensure that all provisions of the legislation restricting the right to freedom of expression in the Cybercrime Law must meet international freedom of expression standards.

ARTICLE 19's analysis of the Cybercrime Law and its recent amendments

ARTICLE 19 notes that the Cybercrime Law contains numerous provisions that violate above mentioned international freedom of expression standards. In particular, we highlight the following problematic provisions:

Vague and overbroad definitions

Chapter 1 of the Cybercrime Law contains several definitions of concepts that are key components of the relevant conducts under the law. The majority of these definitions are vague and overbroad, creating an environment of legal uncertainty for all actors and especially individuals, who are directly impacted by the enforcement of the provisions.

For example:

- Article 4 defines 'informatics' as "means systems, networks, information means, software, computers, the Internet or the like, and related activities thereto." It is unclear what would fall in the categories of 'means systems' or 'Internet or the like' or 'related activities thereto.' This overbroad formulation can easily be abused to attack and punish conducts that are legitimate under international human rights law.

- Another example is 'information' which is defined as **"**data of all kinds that has been processed by any means of information.". Again, the definition is unclear, even though the concept plays a key role in various offences.

- A third striking example is the definition of 'Information Crimes or Cybercrimes' which are intended as "the crimes committed by systems, networks, and information means, software, computers, and the Internet or the like, and the related activities thereto." Once more, this broad wording could be used to punish legitimate activities through which individuals exercise their rights and freedoms, including freedom of expression.

As the definitions in Article 4 play a key role in identifying the conducts which are punishable under the law, the legal uncertainty extends to the latter. In addition, the overly broad and vague formulation fails to provide limits to the discretion of the enforcement authorities.

Problematic provisions on several cybercrimes

Chapter 2 of the Cybercrime Law prohibits several offences, including "illegal access" (Section 5), "interception or capture of data and information" (in Section 8), or "obstructing, disrupting or disabling access to the service" (Section 9). ARTICLE 19 finds that overly broad definitions of these crimes make the purpose of these offences very unclear. As such, they are, or can easily become, unjustified restrictions on the right to receive information under international human rights law. In particular, we note the following:

- Section 5(3) prohibits the "intention to obtain data or information related to the national security of the country, or the national economy, or the structure of communications and sensitive information." A challenge might derive from the formulation of "data or information related to the national security, or the national economy, or the structure of communications and sensitive information." Although national security is a legitimate ground to restrict the right to information, the other elements appear broad. Furthermore, the provision should require that serious harm derives from the conduct criminalised under Article 5(3).

- Section 6 penalises public servants who without authorisation or permission access an information system of the institution in which they work or facilitate another person to access the same. This provision introduces a strict liability offence contrary to Article 2 of the Cybercrime Convention which requires that criminal offences on illegal access must have been committed intentionally. In its current form, the provision fails the test of legality as it leaves discretion to the law enforcement officials to decide what conduct is prohibited. Furthermore, the provisions can be used to punish inadvertent access with no intention to commit a crime. The offence carries a maximum prison sentence of 5 years, which has been increased to 8 years under the Cybercrime Prevention (Amendment Act) 2020, or a fine or both. ARTICLE 19 notes that 8-year imprisonment is not commensurate with the offence given that conduct alone suffices for liability.

- Section 8 prohibits interception or capture of data without permission from the public prosecutor. It does not provide for any intentionality requirement. We observe that Cybercrime Convention in Article 3 (which punishes illegal interception) has several components not present in Section 8 of the Computer Crime Act. The Convention provides for punishing "intentionally, the interception without right, made by technical means, of non-public transmissions of computer data." Hence, we believe that Section 8 should require "dishonest intent" and that interception is done "without right."

- ARTICLE 19 also notes that the relationship between Article 8 (interception or capture of data) and Article 5(3) of the Cybercrime Law should be clarified. It appears that there are substantial overlaps among the two provisions, which could infringe the *bis in idem* principle. Article 8 adds two elements: (i) the absence of permission, which is in line with the Budapest Convention; (ii) it's broader in scope, because it criminalises the interception of all data or information, while data of information related to specific categories (national security, national economy etc.) is treated as a more severe circumstance. To comply with international standards, the provisions should at least specify that the conduct has to be put in place with the dishonest intent and that the data accessed or intercepted are of non-public transmission.

- Section 9 punishes the interference with and damaging of computer data and systems, respectively, without requiring there to be serious damage. We observe that Section 5 of the Cybercrime Convention requires system interference to include "serious hindering without right;" and it only requires that a computer system "fails to operate normally." This is an exceedingly broad provision and could lead to severe punishment of conduct that does not actually cause harm.

Speech offences

Chapters 3, 4 and 5 of the Cybercrime Law punish numerous content-based offences that have nothing to do with preventing cybercrime. These include provoking hatred against foreigners (Section 15), violation of religious beliefs (Section 22), publication of "false news" (Section 24), defamation (Section 25), insults and abuses (Section 26) or numerous 'terrorism' offences (Section 27-29). ARTICLE 19 finds that these provisions do not comply with international freedom of expression standards. In particular:

- ARTICLE 19 has long argued that notes that criminal defamation laws are incompatible with international standards on freedom of expression and should be abolished. The UN Human Rights Committee (that is tasked with interpreting the ICCPR) has similarly urged all States parties to the ICCPR to abolish criminal defamation laws, reflective of an international consensus among international organisations. Such laws rarely can be said to pursue a legitimate aim and be necessary and proportionate.

- The prohibitions of "false news" also violate international freedom of expression standards. As it stands, any Internet user who inadvertently shares a tweet or Facebook post for example that contained false, deceptive, misleading or inaccurate information could be prosecuted under this provision. It would also make the work of the online media outlets susceptible to prosecution. Although media should not aim to report false news; however, an actual prohibition on such news makes the work of journalists covering current developments unreasonably dangerous, as in situations of breaking news facts are often not easy to check. This concerns also the information related to the COVID-19 pandemic. Moreover, it is often open to debate what the 'truth' on a particular matter is and the State should trust citizens to make their own judgement instead of imposing its particular view of events. We also note that the Human Rights Committee and the UN Special Rapporteur on freedom of expression have condemned the use of false news/information provisions in national laws, cautioning that they "unduly limit the exercise of freedom of opinion and expression." The Committee has also clarified that "prosecution and punishment of journalists for the crime of publication of false news merely on the ground, without more, that the news was false [is a] clear violation of Article 19 of the [ICCPR]."

- As for the prohibitions of hatred against sects and groups and regions (Section 14) and hatred towards foreigners in Section 15, ARTICLE 19 recalls that the right to freedom of expression has a broad scope and includes disturbing or provoking expressions, as well as the expression of opinions or ideas that others might find deeply offensive, and this might encompass discriminatory expressions. Therefore, to be criminalised, the use of information or communication networks to engage in 'hate speech' should meet specific thresholds of severity. ARTICLE 19 finds that these provisions fall short of what is required under international law. As noted above, under Article 20 para 2 of the ICCPR, States are required to "prohibit" certain forms of speech which amount to "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence." There is no requirement that these offences are to be committed intentionally; they merely refer to the provocation of contempt or animosity. Nor do they refer to the likelihood of occurrence of violence; rather, Section 14 refers to the endangerment of peace or public tranquillity, which is a substantially broader concept that could be easily instrumentalised to criminalise legitimate behaviours. The terms "advocacy" and "incitement" imply that negligence or recklessness are not sufficient to impose sanctions and that something more than intentional distribution or circulation is required. As currently worded these overbroad formulations pose serious risks of being misinterpreted or abused against the exercise of freedom of expression online. As for Section 15, while the need for a causal link between the conduct and the discrimination or the violence makes the first part of the provision compliant with international standards, the same does not hold true with regards to the overly broad concept of 'animosity.' Therefore, Articles 14 and 15 do not match the thresholds for the punishment of incitement provided by international standards.

- ARTICLE 19 is also concerned that Chapter 4, which prohibits crimes of morality and public order can easily be abused to attack and discourage activists, human rights defenders, journalists and more in general content creators and to censor dissent. Indeed, provisions of Sections 19-25 introduce far-reaching categories of prohibited content, none of which is virtually acceptable under international human rights law. We recall that restrictions on freedom of expression for the protection of public morals must be based on a broad understanding of what 'immoral' means. For instance, Section 19 (prohibiting dissemination and promotion of "indecent" content), is highly problematic as it contains broad and vague concepts of 'disgraceful of modesty' and 'decency'.

Problematic implementation of the Cybercrime Law

ARTICLE 19 also notes that our concerns over these and other provisions are not only theoretical as we are aware that the provisions of the Cybercrime Law have been used to suppress independent journalism and reporting during the pandemic.

Several Sudanese journalists and activists have been persecuted and threatened using the amended Cybercrime law, over publications they posted on social media criticising the authorities. For instance, journalist Mubarak Jumah Musa from Darfur, who was arrested and threatened by the Rapid Support Forces for criticising it; or journalist Adel Keller, who was threatened on-air while interviewing a security adviser during a TV program. A case was opened under his name at the court right after the interview.

Reportedly, from 29-31 May 2020, local authorities harassed journalists Aida Abdel Qader and Lana Sabeel Awad in the Sudanese state of North Darfur as they were reporting on the COVID-19 pandemic. They wrote an investigative piece for *Darfur 24*, which was also posted on the Facebook page "Voluntary Media Development Centre", run by the two women human rights defenders. The report focused on the situation of the COVID-19 virus in the city of Al Fasher, finding that there was a significant shortage of personal protection equipment (PPE) for health workers and criticising the Government for high death rates from the virus in the city, particularly among the elderly. Following the report, the acting governor of North Darfur, Maj Gen Malik Khojali claimed that the local government of North Darfur has been affected by "the unsubstantiated reports regarding the health situation." He said that the reports of the health situation in North Darfur were "exaggerated" and threatened legal action against "anyone publishing false information."

Recommendations

ARTICLE 19 finds that in its current form, the Cybercrime Law is likely to have a chilling effect on freedom of expression and media freedom of Sudan, at a time when access to information is vital. Given the recent restrictions against journalists and the media, the Internet is one of the key spaces for people to share and access information, including the information related to the COVID-19 pandemic. Therefore, to protect freedom of expression online and keep open online space for exercising freedom of expression, we call on the Sudan government to urgently amend the Cybercrime Law and bring it to full compliance with international freedom of expression standards.