BIG BROTHER IS WATCHING: Factors influencing Internet freedom in Africa

By Claudio Butticè

With the possible exception of Kenya and South Africa, Internet freedom is constantly under attack in most African countries. Ethiopia has suffered a dramatic decline in Internet freedom over the past few years, the Ugandan government has imposed a tax on social media, and the Tanzanian government has taken down many websites – a pattern that closely mimics what happens in China and Korea. In a continent where Internet penetration stands at just 31.2 per cent, less than one-third of the population has access to the World Wide Web. Such restrictions on connectivity, as well as a lack of security, online manipulation and disinformation tactics, play a significant role in keeping many countries undeveloped.

Why online manipulation tactics are a threat to freedom

When the Internet started becoming a mainstream technology, many praised it as a liberating force that was helping millions of people to know the truth about the world they lived in. It didn't take much for governments of the less democratic countries to understand the threat it posed to their power. Today, however, even many so-called "democracies" have learned how dangerous Internet freedom can be to their entrenched interests and privileges, and have taken action to disrupt it.

Between 2016 and 2018, Internet freedom was widely abused by many governments to distort the

truth in their favour. Massive online manipulation tactics have been employed in countries such as China, Russia, Syria and Ethiopia. Even Western nations historically known for the independence of their media, such as the United States and Italy, have seen disinformation used to manipulate elections results. Information about many global events, such as the migratory flows from South America and Africa to the United States and Europe, have been distorted to fuel scare-mongering tactics. Governments in all the corners of the world use political and security reasons as excuses to restrict mobile Internet services, especially in areas populated by religious or ethnic minorities. Online dissent has been suppressed by altering, filtering or removing information on social media, and human rights defenders have often been threatened, attacked, or even killed to silence the few independent voices left. For instance, in March 2018, Rwandan blogger Joseph Nkusi was sentenced to 10 years in prison for incitement to civil disobedience and spreading rumours just because he offered a different perspective on the official narrative of the 1994 genocide.

Bots and fake news have been created and deployed to shape the opinion of countless numbers of people. Surreptitious grassroots support for government policies have been fabricated to justify even the most blatant violation of human rights. Many anti-democratic changes have been condoned by building social media bubbles where citizens falsely stand with regimes that are essentially endorsing themselves. And when online news media suffer the same level of restrictions and propaganda that plague the remaining traditional media, any hope for objectivity is lost forever.

Read Also: PARASITES OR PRODUCTIVE WORKERS? The truth about African migrants in Europe

In a nutshell, when people have no access to the truth, or, at least, a different side of the truth, their freedom is stolen, and democracy dies. State-led interventions to restrict Internet freedom ensure that our eyes are open to one thing, and one thing only. Governments that resort to these tactics are scared by the idea of people knowing what is really happening because they have something to hide.

The Chinese influence

It is no mystery why China is the country that is currently spearheading this new wave of policies that aim to chain down Internet freedom. Officials from Beijing are hosting several seminars, conferences and training courses to teach other governments how to monitor and handle negative public opinion. They have devised new tools to "*manage the public opinion in the cyberspace*" and establish a new form of "*socialist journalism with Chinese characteristics*". Similar seminars have been held in the Philippines, Vietnam, India, Lebanon and Saudi Arabia, as well as in many African countries, including Libya, Egypt, Morocco, Tanzania, and Uganda. Unsurprisingly enough, these conferences are often followed by the implementation in those countries of some of the most restrictive and controversial cybercrime and social media laws.

> It is no mystery why China is the country that is currently spearheading this new wave of policies that aim to chain down Internet freedom. Officials from Beijing are hosting several seminars, conferences and training courses to teach other governments how to monitor and handle negative public opinion. They have devised new tools to "*manage the public opinion in the cyberspace*" and establish a new form of "*socialist journalism with Chinese characteristics*".

The Chinese are also the same people who provided all those governments with high-tech surveillance tools to monitor people with no respect for their privacy or human rights. With the excuse of "maintaining public order," autocrats and dictators started employing Artificial Intelligence-powered facial recognition software developed by Chinese companies such as Hikvision and CloudWalk. The latter signed a strategic partnership with the government of Zimbabwe to develop AI that can recognise African faces. Needless to say, the millions of Zimbabwean citizens who saw their personal data sold by the Zimbabwean government to a foreign agency had no say in the deal.

Much of the most important telecommunications infrastructure in these countries is built by China, which apparently doesn't shun any opportunity to collect additional intelligence. In January 2018, much to their dismay, security staff at the African Union found that the computer system in the headquarters that the Chinese government had gifted the organisation was likely a Trojan horse for cyberespionage. Though China officially denied the reports, it appears that the system had been secretly sending data back to Shanghai servers every day for five years. It is not hard to see that there's an agenda behind the Asian giant's digital generosity towards smaller and poorer nations.

Social and blogging media taxes

The Ugandan "social media tax" is a glaring indication that something is wrong. After 32 years of entrenched power held with brutal strength, President Yoweri Museveni found in the Chinese seminars a flawless idea to rule out political opposition without any violence. The Ugandan government imposed an apparently harmless social media tax of 5 cents per day to put an end to "gossip". Citizens who fail to pay the tax will be cut off from social media by their Internet service provider (ISP). In a country where 80 per cent of the population earns less than a dollar a day, five cents a day is no small deal. And since the tax is applied to *all* social media platforms and online messenger services, including Twitter, Instagram, Facebook, Tinder, SnapChat, Tumblr, WhatsApp, Telegram, Viber, Line, and Skype, it quickly adds up. It has been estimated that it could drive up the Internet connection prices to an unacceptable 40 per cent of the average Ugandan's monthly income.

To further enforce this policy, Uganda's Communications Commission Executive Director, Godfrey Mutabazi, suggested telecom companies subject virtual private networks (VPNs) to the tax. In the meantime, ISPs have been ordered to block and switch off VPNs one by one. Banning VPNs is a move that China already tested as a successful tactic to stop those who found a rather simple method to circumvent Internet censorship. It would be a terribly effective way for Museveni to maintain his authoritarian regime without facing the international condemnation that comes with the use of tear gas and live rounds fired at demonstrators. And it could have similar effects as in Cameroon, which restricted Internet access for at least 150 days in 2017.

In 2017, neighbouring Tanzania praised the Chinese government's efforts to replace social media sites such as Facebook and Twitter with "*homegrown sites that are safe, constructive, and popular*". Shortly afterwards, in July 2018, several popular websites had to be shut down to avoid hefty fines imposed by a new troubling law that restricts criticism of the government. In an effort to "*curb*

moral decadence" the government passed a provision that forces bloggers, online streaming platforms, YouTube TV channels, online radio stations, online forums, social media users and Internet cafes to pay a $930 fee to publish online. Bloggers are required to also provide a lengthy list of details and information, while Internet cafés must install surveillance cameras. Violating these new rules or posting anti-government statements on social media may lead to imprisonment for a minimum of 12 months or a fine of at least $2,200, or both. Once again, free expression in Africa was muzzled and curtailed through Internet censorship.

Surveillance and interception of communication

Another way to impose an indirect control on Internet usage is the violation of privacy rights for alleged "security purposes". Many countries, such as Kenya, Uganda, DR Congo and Tanzania, enacted laws that allow the installation of surveillance tools that enable interception of communications with the excuse of "*detecting, deterring and disrupting terrorism*". But who is protecting people from being spied on? Who controls whether these tools are used for surveillance or censorship instead?

In Malawi, the Consolidated ICT Regulatory Management System (CIRMS) – what Malawians call the "Spy Machine" – will allegedly monitor mobile phone service providers to ensure fair pricing and quality of service. Note that "allegedly" here is the key word. Its implementation was initially challenged in the High Court by civil rights movements but the Supreme Court eventually allowed it. Bottom line: the Spy Machine now allows Malawian government officers to listen to subscribers' private conversations with no restriction. To ensure "quality of service", of course.

> Another way to impose an indirect control on Internet usage is the violation of privacy rights for alleged "security purposes". Many countries, such as Kenya, Uganda, DR Congo and Tanzania, enacted laws that allow the installation of surveillance tools that enable interception of communications with the excuse of "*detecting, deterring and disrupting terrorism*". But who is protecting people from being spied on? Who controls whether these tools are used for surveillance or censorship instead?

In Kenya, in January 2017, the Communications Authority (CA) wanted to install a link at the data centre or mobile switching room of mobile operators to identify counterfeit or stolen phones. The purpose of this was supposedly to prevent terrorism in accordance with the provisions of the country's Prevention of Terrorism Act. However, it was later alleged that this system could also intercept phone calls and its implementation was, therefore, blocked by the courts. It was also later alleged that middle boxes may be present on the Safaricom network and that law enforcement officers are allowed to extract private information before seeking a warrant. Other reports purportedly found that the CA procured the Israeli HIWIRE technology to capture, monitor, and analyse private activities on social media. Although all of these allegations are still just allegations and nothing else, it's not hard to understand what the narrative is in this case.

The economic impact of Internet disruptions

Internet shutdowns have become common in sub-Saharan Africa, especially during elections or when public anti-government protests occur. Internet disruptions in the region have occurred in a total combined period of 236 days since 2015. But even if security agencies work with national communications regulators to order the disruptions for purported "national security reasons", many African governments do not even realise how high the cost of these shutdowns is.

In Africa, the information communications technology (ICT) sector is thriving. Over the past two

years, smartphone connections have doubled to almost 200 million, especially in countries such as South Africa, DR Congo, Cameroon, and Kenya. Broadband subscriptions, smartphone purchases, and the mobile money sector are expected to grow exponentially, providing unique opportunities for productivity gains to enterprises and governments. The ICT sector is a potent catalyst of economic growth since it provides the opportunity to overcome Africa's logistical limitations, such as poor road networks and cumbersome bureaucracy. ICTs also allow for a reduction in organisational costs; they speed up the circulation of money, and contribute directly to the economy of many African countries in the form of fees and taxes paid by local and foreign ICT companies. The value added by the ICT ecosystem has been estimated at $10.5 billion in 2016, with an indirect productivity impact worth up to $62 billion.

It is hard to precisely estimate the economic cost of Internet disruptions because every shutdown of communication services affects countless services. Secondary economic damages are suffered by sectors affected by shutdowns, such as call centres, tourism and hospitality services and e-commerce. The Collaboration on International ICT Policy in East and Southern Africa estimates that African governments have suffered a deficit of at least $235 million due to lost tax revenues caused by blocked digital access and reduced worker productivity – a significant sum as the African Union's combined GDP amounts to only $1.5 trillion. Shutdowns represent an insurmountable barrier to business expansion; they damage local competitiveness and erode investor confidence, causing unnecessary reputational risks. In Kenya, the direct and indirect costs of a full Internet shutdown would be among the highest in sub-Saharan Africa, at over $6.3 million per day.

Positive news

Africa's Internet freedom is constantly under attack, but democratic forces are fighting back, and in some instances, were able to score some critical victories.

In May 2018, the Computer Misuse and Cyber Crime Act passed in Kenya provided authorities with the discretion of prosecuting individuals who were found guilty of "subverting national security" while interacting online. While the law purported to protect Internet users from things like cyber harassment, it was clearly created with the sole purpose of muzzling dissenting political views and freedom of expression. But on May 29, the Bloggers Association of Kenya (BAKE) sued the Attorney-General, the Speaker of the National Assembly, the Inspector-General of Police and the Director of Public Prosecution, claiming the Act was unconstitutional. The High Court ruled in favour of the bloggers, suspending 22 provision of the law for further review.

> Shutdowns represent an insurmountable barrier to business expansion; they damage local competitiveness and erode investor confidence, causing unnecessary reputational risks. In Kenya, the direct and indirect costs of a full Internet shutdown would be among the highest in sub-Saharan Africa, at over $6.3 million per day.

Ethiopia, a nation which spearheaded censorship in Africa, is also slowly freeing itself from the draconian restrictions imposed by the 2009 Anti-Terrorism Proclamation. Although strong repressive measures are still present, the newly appointed Prime Minister, Abiy Ahmed, has already started moving towards a more progressive agenda. A gender-balanced cabinet has been appointed, thousands of prisoners, including some prominent bloggers, have been released, dissidents have been allowed to return home, and hundreds of TV channels and websites have been unblocked. Ethiopians are now enjoying an unexpected new age of free expression, which other so-called democracies in the rest of Africa should emulate.

Published by the good folks at The Elephant.

The Elephant is a platform for engaging citizens to reflect, re-member and re-envision their society by interrogating the past, the present, to fashion a future.

Follow us on Twitter.