DATA, THE STATE AND DIGITAL INTRUSION IN NIGERIA

IDAYAT HASSAN

POLICY BRIEF No.5

Published by EISA
14 Park Rd, Richmond
Johannesburg
South Africa
P O Box 740
Auckland Park
2006
South Africa
Tel: 27 11 381 6000
Fax: 27 11 482 6163
Email: eisa@eisa.org
www.eisa.org

© EISA 2022

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of EISA.
First published 2022

Layout and printing by Corpnet, Johannesburg

policy brief

DATA, THE STATE AND DIGITAL INTRUSION IN NIGERIA

Hassan I

CONTENTS

EXECUTIVE SUMMARY 4
WEAK DATA PROTECTION 4
A PUSH FOR LEGISLATIVE CONTROL 5
DIRECTLY LIMITING ACCESS 5
COMPLICIT TECHNOLOGY PARTNERS 6
THE WAY FORWARD 6
REFERENCES 8

EXECUTIVE SUMMARY

The right to privacy is a fundamental human right guaranteed by international human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR). It is embedded in the African Union's 2014 Convention on Cybersecurity and Personal Data Protection and is guaranteed in Sections 37 and 39 of the 1999 constitution of Nigeria as amended, which guarantees the rights to privacy[1] and freedom of speech and expression.[2] However, the practical application of these provisions is increasingly problematic, with governments using them to constrict civic space and quash dissent, particularly in the digital realm.

Social media has granted Nigerians the power to participate in governance processes, hold elected officials accountable, make business transactions and engage with friends and family at home and abroad. Key examples include the use of online platforms for business operations and learning during the Covid-19 lockdowns. Information about the pandemic was also channelled through social media handles run by government bodies such as the National Centre for Disease Control (NCDC).

At the same time as the use of internet increased during the Covid-19 lockdown period, digital attacks were on the rise, with civil society and media institutes targeted. Rather than protecting citizens' freedom of expression online, the Nigerian state has used the pretext of national security to clamp down on individual and collective voices. Musa Babale Azare[3] is one example of a citizen detained by police for criticising elements of the state online – in his case the then Bauchi state governor, Muhammad Abdullah Abubakar. The 2020 #ENDSARS protests that spread to more than half the states in the federation, relied heavily on online networks to mobilise. In response, the government embarked on a legislative push to regulate social media in a way that would allow law enforcement to shut down specific platforms and the internet.

Even without the legislation in place, the government has acted. Twitter was officially banned in May 2021 for taking down a tweet by President Buhari that it claimed violated its terms of reference. It can be surmised that twitters role in fuelling #EndSARS protests, may have contributed to the government's decision to officially ban Twitter. China's approach to digital surveillance appears to be a model that Nigeria not only admires but is interested in emulating. After the Twitter ban was announced it emerged that Nigerian government officials had been in talks with the Cyberspace Administration of China, which supports the state in directly controlling and regulating its cyberspace. While exercising this level of control may seem unlikely in Nigeria, in the current context, digital freedoms and data privacy remain under serious threat in four main areas.

WEAK DATA PROTECTION

The Nigerian state is collecting more data about its citizens through the expansion of voter registration, mobile phone sim card registration, the creation of abiometric verification numbers and the digitisation of passport and driver's licence registrations. This data is collected and held by different government agencies with limited capacity to monitor and protect it against threats from hackers and unscrupulous private entities. Thousands of employees across many offices can access the databases, cybersecurity is often weak and when privacy breaches do occur, they are not usually treated seriously by data protection authorities, which lack the capacity and budgets to function effectively.

To offer some level of protection to Nigerians' data online, the Nigeria Data Protection Regulations (NDPR) were introduced in 2019. A breach of the NDPR can attract a fine of between N200,000 ($555) and N500,000 ($1,367), imprisonment of three years, or both. To date, its implementation has been negligible and the NDPR does not cover the protection of personal data, regulate processing or grant protection against harmful data rules, and has jurisdictional challenges. The fact that the NDPR is a regulation[4] and not an act of parliament also limits its effectiveness in such an important area. As a relatively new regulation, there has not been much application of it, or any evidence that companies are willing to comply with it.

The lack of attention given to personal data protection in Nigeria is worrying given the way in which data can be used and abused for electoral gain in elections. Data-driven campaigning in Nigerian elections is growing in prominence. Generally, political actors use data and digital technologies to fundraise, test for the resonance of campaign messages, target messages to specific geographic locations, and send out bulk SMS, audio, and WhatsApp messages. All these can be designed to sway voters with greater granularity, speed and at a larger scale.[5] The problem is not just confined to elections. The way in which these firms acquire the data of citizens and how they use it should be of concern to the state. Newly established digital loan companies are violating subscribers' rights by breaching rules on data privacy and resorting to cyber bullying to get defaulters to make repayments.[6]

[1] Section 37 provides: "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected."
[2] Section 39 provides that every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and even own and operate a media organisation.
[3] https://dailytrust.com/amp/policemen-arrest-blogger-in-abuja-for-criticising-governor
[4] https://ndpr.nitda.gov.ng/
[5] Tactical Tech, Personal Data: Political Persuasion. Inside the Influence Industry. How it works.
[6] https://www.premiumtimesng.com/news/headlines/499999-investigation-how-digital-loan-providers-breach-data-privacy-violate-rights-of-nigerians.html

A PUSH FOR LEGISLATIVE CONTROL

Social media regulations have been used to stifle, regulate, and monitor freedom of speech and expression across Africa. Over the last five years, Nigeria has attempted to create new laws that limit digital freedom. The new laws go beyond the provisions outlined in the Cybercrime Act (2015), which punishes fake news by a jail term of three years, a N7million ($13,000) fine, or both. The Act also prohibits the distribution of racist and xenophobic material to the public through a computer system or network and the use of threats of violence and offensive statements to persons based on race, religion, colour, descent or national or ethnic origin.

In November 2019 the Protection from Internet Falsehood and Manipulation Bill, popularly known as the "Social Media Bill", was tabled at Nigeria's House of Representatives. The Bill seeks to tackle the increasing problem of false information, but in doing so it poses a severe threat to Nigerians' democratic right to freedom of speech. It contains draconian provisions which, if made law, would empower the Nigerian government to unilaterally shut down social media and possibly the internet for posts deemed to pose risks to public safety and national security. Yet the vague definitions of what constitutes public safety or national security would open this up to political influence.

Furthermore, there is a low burden of proof in the determination of contraventions of its provisions. The Bill provides for subjective judgement as to whether the transmission of false statements of fact is likely to, amongst other things, incite feelings of enmity or hatred towards a person, or ill-will between groups of persons. It is to be implemented and enforced by an overburdened, under-resourced and digitally apathetic Nigeria Police Force.

Finally, the exercise of "targeted correction regulation" proposed by the Bill would go against best-practice data privacy principles, as directing internet intermediaries to send correction notices to all end-users who accessed a false statement or subject material via their platform can amount to an unethical tracking of users. Although the bill was not passed and remains shelved as at the time of writing, there is a likelihood it could come back in a revised format.

Also in 2019, the Prohibition of Hate Speeches and For Other Related Matters, otherwise known as the "hate speech bill", was reintroduced into the Senate. The Bill seeks to prohibit inter alia hate speech, discriminatory language, and harassment based on ethnicity. It has received extensive criticism amidst concerns that it will impede the freedom of expression as provided for under section 39 of the Nigerian constitution and contravenes international law. Critics argue that problematic definitions of what constitutes free speech versus offensive speech means that if passed into law it will provide cover for the government to attack free speech and prevent rights organisation and the media from effectively performing their functions. With extremely harsh punitive sanctions proposed the have had a chilling effect on the freedom of digital expression in Nigeria, but it failed to pass due to citizen agitation and remains in abeyance for now.

A third piece of legislation that could fundamentally reshape the digital landscape is the amendment to the extant Nigerian Broadcasting Commission (NBC) Act. The new amendment, which is still being developed, is set to include new functions such as the regulation of social media, digital traffic regulation and monitoring of internet broadcasting. It would grant the NBC power of access to the back end of social media platforms and online content providers for "easy facilitation of complaint resolution". Importantly, the proposed amendment will empower the commission, police and other security agencies to request personal user information for ongoing investigations. In a captive society such as Nigeria where political pressure can be applied to the NBC or any of the other agencies, in a partisan or restrictive way, the provisions outlined in the bill are dangerous.

What is notable is that the drafts of all three proposed pieces of legislation signal an attempt to provide the government with access to the personal data of citizens. There is a risk that government institutions could act in a partisan manner and further restrict freedom of expression online. Instead of focusing on regulations, the Nigerian government should focus on regulating the tech companies under a carefully worked out framework. This framework should address issues of content moderation, transparency around political advertising and maintaining a physical presence in the country.

DIRECTLY LIMITING ACCESS

Nigeria has not experienced a nationwide internet shutdown, however, Zamfara State did experience a full internet and mobile network blackout in 2021, as part of ongoing military operations.[7] Specifically, select social media sites were banned for months (Twitter) and some individual websites were blocked or taken down. In November 2020, the website of the Feminist Coalition, radioisiaq.com, and endsars.com were blocked. The websites, which remained inaccessible on mobile networks as of July 2021, belonged to organisations that played prominent roles during the #EndSARS protests. Online newspaper and whistleblowing platform the Peoples Gazette saw access to its site for MTN and 9Mobile users restricted after it published several scoops about proceedings at Aso Rock, Nigeria's seat of power.

[7] https://guardian.ng/news/zamfara-residents-lament-indefinite-telecoms-shutdown-amid-rise-in-bandits-activities/

Twitter's decision to delete a tweet by President Muhammad Buhari that broke community guidelines saw the federal government move quickly to block access to the application in May 2021. The role of the platform in mobilising and organising during the October 2020 #ENDSARS protests combined with CEO Jack Dorsey's own tweets in support of the protest and directing people to the GoFundMe account of the Feminist Coalition was also behind this decision. For seven months citizens could not access the platform without using a virtual private network (VPN) until an agreement was reached between the company and the federal government. While the full terms of the deal with Twitter are not in the public domain, they allegedly include enrolling Nigeria's law enforcement agencies in Twitter's Partners Support Portal[8] and ensuring that fake and harmful content is removed in a timely manner. This has led to concerns that the agreement with Twitter could lead to an increase in the removal of content, a stifling of free speech and increased crackdowns on Twitter users and activists.

Although Twitter is now accessible, the "Twitter ban" reiterated the fact that whilst social media applications are an accessible tool for civic advocacy, the centralised nature of the technology platforms means that they can be easily censored and blocked by authoritarian regimes.

COMPLICIT TECHNOLOGY PARTNERS

Tech companies are complicit in the mismanagement of user data, which has real-life consequences for users, especially in developing countries like Nigeria. Facebook's entire operating model is based on collecting and then selling its users' data. The platform has a huge amount of information about every activity on its network and this can in part explain its continued push to grow an African user base through initiatives such as Free Basics.[9] Some of this data can be handed over to governments and law enforcement agencies when requested. This is potentially problematic in states where investigative institutions are politically partisan or seek to clampdown on dissenting voices. Google, Facebook and Twitter have all received and handled requests from Nigeria about subscribers' data, content preservation and content removal. A 2017 CIPESA[10] report revealed Nigeria made requests regarding 113 Facebook accounts, the highest number of requests from an African country.

Telecommunications providers are also suspected of sharing user data with law enforcement agencies. They are compelled to do so more by political pressure than a clear legal requirement. In 2020, Babatunde Olusola was picked up and detained for operating a "parody account" of the former president, Goodluck Jonathan. His capture appears to have been aided by the police gaining access to his call log record from the telecommunications provider, from which they tracked down his uncle, who was then co-opted into aiding his arrest.

These forms of digital intrusion are further complemented by mass surveillance of internet and phones. In the states of Bayelsa and Delta, governors have been accused of acquiring surveillance systems that can track the exact position of users and decrypt telephone calls made between them. This technology has been used to track down real and perceived opposition.[11] The Nigeria government has also invested in mass surveillance equipment, including a communication system that tracks calls and SMSs. The provision of WhatsApp Intercept Solution and Thuraya Interception Solution was provided for in a supplementary budget granted to the National Intelligence Agency less than a month after the #ENDSARs protest against police brutality in Nigeria.[12] There are growing concerns that these are being utilised to spy on media, civil society and political opponents as much as criminal elements of society.

THE WAY FORWARD

Nigerians' digital rights and data are poorly protected and under threat. Apart from limiting the rights of citizens to receive and impart information on select social media platforms, the government has taken a heavy-handed approach to regulation of digital platforms that risks reducing further the space for dissenting digital voices in Nigeria. The legislative push has also been in this direction, when the focus should be on establishing an environment that better supports the protection and privacy of Nigerians' data, especially from partisan institutions and actors.

Robust data protection laws that protect and not inhibit the rights of citizens are critical, however, it is also important to capacitate agencies that are charged with enforcing the provisions on all private sector actors. Furthermore, civic education and engagement initiatives should emphasise the importance of protecting personal data and explaining the role of legislation. To further support citizen engagement, a mechanism through which they can raise complaints is needed.

Digital authoritarianism is a growing concern in Nigeria and telecommunications companies and social media platforms must not be seen to be complicit in such actions. At the same time social media companies can do more to moderate content and take down posts that promote hate speech in the commonly spoken languages of Nigeria.

To counteract government censorship and surveillance collaborative action is needed. This can be led by civic activists and media organisations at national, regional and continental level. Identification and sharing of best practices for protecting internet freedom will be critical, especially in the run up to elections, as this is when constriction of the digital space is particularly prevalent.

[8] https://www.bbc.com/news/world-africa-60024742
[9] https://journals.sagepub.com/doi/full/10.1177/0163443719890530
[10] https://qz.com/africa/1064168/african-governments-user-data-requests-from-facebook-google-and-twitter-hits-historic-level/
[11] https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html
[12] https://www.premiumtimesng.com/news/headlines/473147-as-nigeria-moves-to-control-media-nia-gets-n4-8bn-to-monitor-whatsapp-phone-calls.html

References

Adepetun, A., Unukaso, F., Akhaine, S., & Alabi, A. 2021. Zamfara residents lament indefinite telecoms shutdown amid rise in bandits' activities. https://guardian.ng/news/zamfara-residents-lament-indefinite-telecoms-shutdown-amid-rise-in-bandits-activities/

DailyTrust. 2016. Policemen arrest Blogger for criticising governor. https://dailytrust.com/amp/policemen-arrest-blogger-in-abuja-for-criticising-governor

Emmanuel, O. 2016. INVESTIGATION: How Governors Dickson, Okowa spend billions on high tech spying on opponents, others. https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html

Iroanusi, Q. 2021. Nigerian govt moves to control media, allocates N4.8bn to monitor WhatsApp, phone calls. https://www.premiumtimesng.com/news/headlines/473147-as-nigeria-moves-to-control-media-nia-gets-n4-8bn-to-monitor-whatsapp-phone-calls.html

Kazeem, Y. 2022. African governments are requesting more user data from Facebook, Google, and Twitter than ever before. https://qz.com/africa/1064168/african-governments-user-data-requests-from-facebook-google-and-twitter-hits-historic-level/

National Information Technology Development Agency. 2020. Nigeria Data Protection Regulation. https://ndpr.nitda.gov.ng/

Nothias, T. 2020. Access granted: Facebook's free basics in Africa. https://journals.sagepub.com/doi/full/10.1177/0163443719890530

Orjinmo, N. 2022. How Nigeria succeeded in clipping Twitter's wings. https://www.bbc.com/news/world-africa-60024742

Tactical Tech. 2019. Personal Data: Political Persuasion: Inside the Influence Industry, How it Works. Tactical Tech. Berlin.

Notes

POLICY BRIEF NO. 5 | DATA, THE STATE AND DIGITAL INTRUSION IN NIGERIA
THIS POLICY BRIEF IS PART OF EISA'S DIALOGUE SERIES ON TECHNOLOGY AND DEMOCRACY IN AFRICA

Notes

About EISA

Since its inception in July 1996 EISA has established itself as a leading institution and influential player dealing with elections and democracy related issues in the African continent. EISA has past and/or current field offices in 20 African countries. The organisation's Strategic Goals are:

- Electoral processes are inclusive, transparent, peaceful and well-managed;
- Citizens participate effectively in the democratic process;
- Political institutions and processes are democratic and function effectively; and
- EISA is a stronger and more influential organisation

The vision of EISA is "an African continent where democratic governance, human rights and citizen participation are upheld in a peaceful environment". This vision is executed through the organisational mission of "striving for excellence in the promotion of credible elections, participatory democracy, a human rights culture, and the strengthening of governance institutions for the consolidation of democracy in Africa".

Having supported and/or observed over 100 electoral processes in Africa, EISA has extensive experience in formulating, structuring and implementing democratic and electoral initiatives. It has built an internationally recognised centre for policy, research and information and provides this service to electoral management bodies, political parties, parliaments, national and local governments and civil society organisations in a variety of areas, such as voter and civic education and electoral assistance and observation. Besides its expanded geographical scope, the Institute works in the in-between election areas along the electoral and parliamentary cycle, including constitution building processes, legislative strengthening, conflict management and transformation, political party development and strengthening and supporting capacity building for members of parliament and parliamentary structures. EISA also provides technical assistance to continental and regional inter-governmental institutions, Election Management Bodies and Civil Society Organisations.

14 Park Road Richmond
Johannesburg 2092, South Africa
P.O. Box 740 Auckland Park 2006
Tel: +27 11 381 6000-7
Fax: +27 11 482 6163
Email: eisa@eisa.org
www.eisa.org

This publication and series are made possible through the generous financial support of the Government of Sweden through the Swedish International Development Cooperation Agency (Sida).