DATA, THE STATE AND DIGITAL INTRUSION IN NIGERIA

IDAYAT HASSAN

EISA
Electoral Institute for Sustainable Democracy in Africa

POLICY BRIEF No.5
DATA, THE STATE AND DIGITAL INTRUSION IN NIGERIA

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

Hassan I

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
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 Section 37 of the Nigerian Constitution and in Section 6 of the Nigerian Information and Communication Technology Act (CITCIA) as amended in 2019. The right to freedom of expression is also guaranteed under Article 19 of the ICCPR. However, the practical application of these provisions is increasingly problematic, with governments using them to constrain civic space and quash dissent, particularly in the digital realm.

Section 37 provides: "The privacy of the citizen, his correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected. No person shall be compelled to disclose his sources of income or to answer questions relating to such income." Section 6 of the CITCIA provides: "Personal data shall be protected against unlawful collection, use, disclosure or retention. No person shall be required to disclose any information of a personal nature to any person, government, or public authority." The right to freedom of expression is also protected under Section 19 of the Nigerian Constitution, which states: "The freedom of expression includes the freedom to hold opinions and to receive and impart information and ideas through any media and不论 by any means."

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 biometric registration systems, national identity card, passport and driver’s licence registrations. This data is collected and held by different government agencies with limited capacity to monitor it and hence protect it from hackers and unscrupulous private entities. Thousands of employees across many offices can access and engage with 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, 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 in the context of data protection and information security, harmful data rules, and jurisdictional challenges. The fact that the NDPR is a regulation 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, combined with the fast pace at which data is being used and abused for electoral gain in elections. Data-driven campaigning in Nigerian elections is growing in prominence as big 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, specifically targeting people and groups of people and thus more refined than ever. The elections in which these firms can be used to sway citizens in a manner that is not limited to the platform they access false information on their platforms can amount to an unethical tracking of users.

DATA, THE STATE AND DIGITAL INTRUSION IN NIGERIA

The Nigerian government, seeking to prevent the transmission of false statements of fact is likely to do so by overburdening and under-resourced and digitally apathetic Nigerian Police Force. The lack of a clear definition 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 do so by overburdening and under-resourced and digitally apathetic Nigerian Police Force.

A FINAL WORD

The bill 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 to easily facilitate other measures which would open this up to political influence. The GDPR’s enforcement framework. This framework should address issues of corporate accountability and power balances, including with respect to the personal data of citizens.

The Nigerian government should focus on regulating the tech companies under a carefully worked out framework. It is to be implemented and enforced by an overburdened under-resourced and digitally apathetic Nigerian Police Force.

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 do so by overburdening and under-resourced and digitally apathetic Nigerian Police Force.

The lack of a clear definition of what constitutes public safety or national security would open this up to political influence. The lack of a clear definition of what constitutes public safety or national security would open this up to political influence.

Nigeria has not experienced a nationwide internet shutdown, however, Zamfara State did experience a full internet shutdown for access to its site for MTN and 9Mobile users restricted as part of ongoing military operations. Similarly, select social media sites were banned for months (Twitter, Facebook, Instagram) and then restored. The Nigerian government should focus on regulating the tech companies under a carefully worked out framework. It is to be implemented and enforced by an overburdened under-resourced and digitally apathetic Nigerian Police Force.

The Nigerian government should focus on regulating the tech companies under a carefully worked out framework. This framework should address issues of corporate accountability and power balances, including with respect to the personal data of citizens.

The Nigerian government should focus on regulating the tech companies under a carefully worked out framework. This framework should address issues of corporate accountability and power balances, including with respect to the personal data of citizens.

The Nigerian government should focus on regulating the tech companies under a carefully worked out framework. This framework should address issues of corporate accountability and power balances, including with respect to the personal data of citizens.

The Nigerian government should focus on regulating the tech companies under a carefully worked out framework. This framework should address issues of corporate accountability and power balances, including with respect to the personal data of citizens.
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 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. 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 clamp down on dissenting voices. Google, Facebook and Twitter have all received and allowed requests from an African country.

Digital authoritarianism is a growing concern in Nigeria, with platforms that risks reducing further the space for 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 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.

Digital authoritarianism is a growing concern in Nigeria and telecommunication 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.

### THE WAY FORWARD

Nigerian’s 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 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.

Digital authoritarianism is a growing concern in Nigeria and telecommunication 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.
References


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.