The Role of Courts in Safeguarding Africa's E-commerce Environment

By:

Michael Asiedu

December 04, 2022

Africa’s projected revenue for its e-commerce market would be US$43.89bn by the end of 2022. With an annual growth rate of 18.07%, the market volume will stand at US$72.24bn by 2025. Likewise, in the e-commerce market, the number of users is expected to increase from 387.8m to 519.4m users by 2025.

Essentially, e-commerce is serious business! However, while the prospect of this growth is exciting; weak and fragmented regulation in areas such as consumer, data and privacy protection across African countries is a concern that cannot only derail growth but also risk enabling those in control of resources and political power, i.e., big companies and governments to configure the digitalization process to their interests.

Taking a cue from trade agreements, the four main categories relevant for organizing e-commerce under the African Continental Free Trade Area (AfCFTA) would deal with market access; rules and regulations; issues surrounding facilitation; and enabling issues. Market access would largely deal with

difficulties that may arise, for instance, custom duties in terms of cross border transactions, valuation, and pricing of products, etc. Rules and regulations concern legal arrangements that would have a bearing on e-commerce, i.e., data protection, competition policy, issues related to tax as well as intellectual property rights.

Facilitation covers ways to make e-commerce efficient through efforts such as digital identity, cyber security, etc. Enabling issues captures the structural foundation that will make a vibrant digital economy such as ease of internet access, affordability in addition to other technology-related infrastructure.

In this short paper, I demonstrate an already emerging role of courts in categories such as rules and regulations, facilitation and enabling issues. Four cases with direct relevance to e-commerce have been painstakingly chosen to reflect the significance of courts and their rulings. The first case is the second challenge of Sudan's internet shutdown by Lawyer Abdel-Adheem Hassan on behalf of Sudan's Customer Protection Agency and citizens at large. While about 12 cases of internet shutdowns have received court rulings this one is chosen because its challenge in court was not only left for human rights and digital rights groups but a consumer protection agency with economic concerns for the shutdown got involved too. Also, when it comes to e-commerce, issues of consumer protection and internet access are non-negotiable provisions.

The second case deals with a data protection ruling given by the highest court in Kenya, a case which also cuts to the core of e-commerce because data protection as well as data privacy issues form the bedrock of e-commerce operations. The third and fourth cases deal with digital banking and financial payment platforms giving credence to the instrumental role such outfits play in any e-commerce activity. While these cases are scrutinized in the context of their respective countries, Sudan, Kenya, and Uganda, each of these "precedent setting cases" have a bearing on how stakeholders including both clients/consumers and service providers can begin to perceive matters surrounding the courts and its contribution in making e-commerce a success particularly on the African continent.

The digital economy thrives through a web of complex contractual and noncontractual relationships between actors including consumers, businesses

(service providers) and governments. This is first made possible through an enabling environment with technology and access to internet infrastructure. Essentially, there is no digital economy without internet access, hence, Sudan's customer rights internet shutdown litigation becomes significant.

Sudan: *Abdel-Adheem Hassan, Sudan Customer Protection Agency v Zain Telecom*:

Sudan's Internet Shutdown and Customer Rights Litigation

On 23 June 2019 Lawyer Abdel-Adheem Hassan won a case against Zain Telecom in Sudan for cutting off internet access at the instruction of Sudan's military rulers (BBC 2019). He argued in court that "the operator failed to provide written orders to disconnect the internet". He took the case to court in his personal capacity as a customer of Zain Telecom. Lawyer Hassan won his case and became the only individual with internet access from Zain Telecom without resorting to complicated maneuvers at a point in Khartoum. He subsequently went to court on behalf of Sudan's Customer Protection Agency to seek a court order which led to the restoration of internet access as the internet had affected economic activities.

Elsewhere, in Nairobi, Kenya; the fate of a data instrument (digital-biometric ID card) was being decided.

Kenya: **Data Privacy Case:**

Nubian Rights Forum et al. v. the Honourable Attorney General of Kenya et al.

Other interested parties included: Kenya Human Rights Commission (KHRC), and the Kenya National Commission on Human Rights (KNCHR).

In October 2021, the highest court in Kenya declared illegal the rollout of the country's biometric identification (ID) system known nationally as Huduma Namba (BBC 2021). In the decision, Justice Ngaah ruled that the Data Protection Act of 2019 which was operationalized in 2020 should be applied retroactively to the government's rollout of its (National Integrated Identity Management System-NIIMS) which was begun in November 2020. Significantly, the judge indicated that the initiative, Huduma Namba was not in alignment

with Kenya's 2019 Data Protection Act.

The same court had in 2020 halted the rollout of the biometric IDs until there were proper data protection laws. It was at the backdrop of this ruling that in November 2020, Kenya passed its data protection law which complied with European Union (EU) legal standards as part of its efforts to attract investment in its information technology sector.

In Justice Ngaah's ruling, he further faulted the government for not doing an assessment of how data protection would be impacted before the rollout of the biometric ID system given that sensitive information such as contact details, fingerprints and a person's profession were collected in 2019. Eventually, while Justice Ngaah ruled that Kenya's biometric ID move was constitutional, the crux of the matter was how data-sensitive information about individuals would be protected.

Significance of These Two Rulings: Sudan and Kenya

When you consider these two court rulings it becomes obvious that it would be a frightful scenario should consumers (customers) or citizens be left with weak regulation. If such a scenario festers, it could both curtail consumer participation and erode trust and enthusiasm. The AfCFTA E-Commerce Protocol is therefore a welcome instrument.

At the onset, if e-commerce is to succeed and fulfill its economic potential, legal systems do need to accommodate emerging business practices that are digitally inclined for instance, digital payment platforms, small scale online shops etc. Therefore, in terms of internet access and connectivity, it was vital for Sudan's Customer Protection Agency to champion the country's internet shutdown litigation-the message here is clear, no internet access no digital business activities.

On data privacy, digital identity programs provide a unique opportunity for increased inclusivity, better financial participation and wider access to government resources and initiatives. Lack of access is not only an African problem, in fact over a billion people have been classified as invisible due to lack of any form of identification. That is why governments must ensure that proper data protection regulations surrounding privacy, security and logistics

are observed. Again, this is crucial since the harvesting of personal data by both governmental and private entities is on the increase. Essentially, the ruling by Kenya's court is a signal to authorities around the globe to ensure that necessary systems that will guarantee the security of citizens' data and its compliance with best human right standards are implemented.

Financial Payments and Digital Banking Platforms

Uganda: ***Digital Banking Fraud Case: Aida Atiku v Centenary Bank***

Another significant case that could have impact on e-commerce in Africa is that of Aida Atiku v Centenary Bank in Uganda, the case was decided in July 2022. Aida Atiku the Plaintiff had sought a decision from the Commercial Division of the Kampala High Court in Uganda. Ms. Atiku had opened an account with the Centenary Bank in 2020 with Shs56.3m as deposit. In her court application she indicated that she had withdrawn only Shs700,000 of the total amount deposited.

After eight months, she had returned to the bank to withdraw the rest of her money but found the account empty-there was no money in the account triggering a case of digital fraud which could happen especially as e-commerce expands and advances across Africa continent. A key question that arises is who bears responsibility for digital fraud? Is it money transaction or payment platforms such as banks or "FinTechs". How do we safeguard privacy related information such as user IDs, passwords and confidential PIN numbers needed for online transactions? The bottom line is account takeovers especially online occur when persons (fraudsters) other than the legitimate user (owner) acquire these login details and access the account as their own.

In ruling on the case on 18 July 2022, Justice Stephen Mubiru decided that it is the "customers responsibility to always keep their banking information such as user IDs, passwords, and PIN numbers confidential". This effectively shifts the blame on digital fraud to bank clients, however, there is a caveat. Justice Mubiru held this blame and responsibility on clients to be valid when the bank can show that its security procedure has a commercially reasonable method of providing security against unauthorized payment orders.

The court also held that financial institutions offering mobile banking have the obligation to offer secure platforms for their customers to safely conduct their banking online. Among the other responsibilities of banks in this regard were: banks were to establish robust fraud detection and prevention mechanisms, update digital banking technology, identify suspicious transactions and trace, track and verify transactions over their digital banking platforms. Added to these other parameters include, banks notifying clients of updated information on how to access digital banking services including details about their customer ID, choosing appropriate passwords as well as further authentication or security options. On issues of elderly citizens, the court added that special interventions should be taken to assist elderly citizens. Kenya: Alleged Money Laundering:

Kenya Asset Recovery v Flutterwave Payments Technology Ltd

Another prominent case which has not been decided yet is that of an alleged money laundering involving Flutterwave Payments Technology Ltd Kenya. Here, a Kenyan High Court has frozen about 43 million dollars held in 52 multi-currency accounts in three Kenyan banks belonging to Flutterwave. This order was sought by Kenya's Assets Recovery Agency and granted by Judge Esther Maina. Justice Maina said in her ruling that, "these orders shall subsist for a period of 90 days according to section 84 of Proceeds of Crime and Anti-Money Laundering Act,". Kenya-registered Fluterwave Payments Technology Ltd which denies this claim of financial impropriety as "entirely false" can therefore not transfer nor withdraw the funds according to the court order. Flutterwave is Africa focused and specializes in individual and consumer financial transfers and hence one of the platforms facilitating and capitalizing on e-commerce transactions in Africa. This court order took effect from 1 July 2022.

Significance of these two Cases:

What the ruling on *Aida Atiku v Centenary Bank* effectively demonstrates is that in instances of digital fraud on banking platforms, the loss is borne by the party who could have most prevented it. Thus, if the bank security was sufficient, the customer bears the responsibility. While it remains to be seen whether this case is appealed or challenged further, it leaves clients vulnerable especially on determinations of what is sufficient security provided by banks and payment platforms especially in Africa.

On Flutterwave, while FinTechs would be important bridge in payment facilitation in addition to traditional banks, such outfits must be regulated check issues of illicit financial flows or financial impropriety.

Suggestions going forward

There should be a constant flow in terms of access to the internet; its economic impacts are dire. For instance, for 3 hours of internet shutdown in Sudan in 2021, 13.2 million people were affected with an economic loss of $1.2 million mostly affecting small businesses online (Statista 2022). Essentially in terms of internet access and connectivity, for the purposes of e-commerce, there should be a law that ensures access unless in extreme circumstance where a country's national security is genuinely under threat. Here respective legislative bodies must in consultation with business governing bodies clearly outline what those measures should be.

Also on data privacy, data protection should form the basis of all e-commerce transactions. Many African countries would continue to embark on biometric identification or digital identification processes, what the ruling from Kenya has emphasized is that data protection should be paramount, hence, this ruling becomes a towering precedent which can shape the legal discourse not only across the sub-region but in other jurisdictions around the globe as well.

Digital banking and payment platforms must be made through legal arrangements in negotiating the AfCFTA e-commerce protocol to bear the most responsibility in safeguarding client information particularly in terms of the overall security architecture, thus be quick to track and trace instances of fraud and potential fraud, quick prompts to legitimate account owners etc.

Conclusion

In the light of the many issues that will come up in e-commerce activities on the continent; it is important not to relegate the role of the courts to the background. These two rulings have already demonstrated the courts would play a role and this role would be instrumental, particularly also in jurisdictional determination when breaches surrounding the e-commerce environment occurs. Michael Asiedu Michael is a doctoral researcher at the University of St.Gallen Institute of Political Science. His research focuses on Technology

(Internet) and its impact on Africa. His current research examines the role of courts in responding to to internet shutdowns in Africa.

Michael Asiedu is a doctoral researcher at the University of St. Gallen Institute of Political Science. His research focuses on Technology (the Internet) and its impact on Africa. His current research examines the role of courts in responding to internet shutdowns in Africa.

View online: The Role of Courts in Safeguarding Africa's E-commerce Environment

Provided by Afronomicslaw