AFRICAN JOURNAL OF LEGAL ISSUES IN TECHNOLOGY AND INNOVATION

VOLUME 1, NUMBER 1, 2023

A peer reviewed publication of the
International University of East Africa
Faculty of Law

EDITORIAL BOARD

TYPESETTING AND ARTWORK

INTERNATIONAL UNIVERSITY OF EAST AFRICA

TABLE OF CONTENTS

FOREWORD

As we move towards the Fourth Industrial Revolution (4IR), the legal industry must rapidly adapt and adopt new technologies and advancements that are transforming the way the world works. Today, legal practitioners must deal with cases that touch on complex technologies such as autonomous systems, artificial intelligence, machine learning, cross-border digital data, software code usage, intellectual property rights, digital rights management and a panoply of other areas where technology, work and society intersect. Even a casual review of the legal cases that have been and are being adjudicated worldwide makes it abundantly clear that understanding the intersection of law and technology is a *sine qua non* for legal professionals going forward. The profession can either choose the way to obsolescence and irrelevance by doing nothing or by sticking to the ways of the past or it can become relevant by reinventing the present and the future.

I am thrilled that the International University of East Africa's inaugural African Journal of Legal Issues in Technology and Innovation is embracing the future. The Journal reinvents the present and the future by providing a platform for legal experts, technologists and innovators to explore the cutting-edge trends, innovations and challenges that are shaping the present and the future of law, technology and society.

The Journal aims to be a valuable resource for all those who are interested in the intersection of law and technology, whether they are practicing attorneys, law students, legal tech entrepreneurs or anyone interested in the legal industry. By providing in-depth analyses, expert insights and practical advice, this Journal can help readers be part of the rapid changes that define the era and enable readers to stay ahead of the curve.

In this Journal, you will find articles that cover a wide range of topics related to law and technology, including artificial intelligence, blockchain, e-discovery, legal project management and much more. By exploring these topics, readers can gain a deeper understanding of the potential benefits and risks associated with the use of new technologies in the legal industry.

There have been several landmark cases, in Africa and abroad, in which knowledge of technology has played a key role in shaping legal outcomes. For example, in 2019 a Zimbabwean court used facial recognition technology to identify individuals who participated in a violent protest. The court used footage from security cameras to identify the protesters, and several individuals were convicted based on this evidence. In 2013 (and in subsequent years), Kenya's electoral Commission used biometric voter verification technology to prevent voter fraud during the country's presidential election. The Commission required all voters to have their fingerprints scanned before casting their ballots, which helped to ensure the integrity of the election. In 2016, a South African court allowed a virtual witness to give evidence via video link in a murder trial. The witness, who lived overseas, was able to testify remotely using video conferencing technology. In 2018, a Nigerian court used digital evidence in a corruption case against a former governor. The court admitted bank statements, financial records and email correspondence as evidence, which helped to secure the conviction of the defendant. In 2020, a Rwandan court used drones to deliver justice to remote areas of the country. The court used drones to transport legal documents and evidence to

areas that were difficult to reach by road, which helped to ensure that justice was delivered to all citizens, regardless of their location.

Further afield, similar cases have hinged on knowledge of technology. Take *Riley v. California* (2014): in this case, the United States' (US) Supreme Court ruled that police officers must obtain a warrant before searching a suspect's cell phone. *United States v. Microsoft* (2018): in this case, the US Supreme Court ruled that Microsoft could not be compelled to turn over customer data stored on servers located overseas to the U.S. government. The court found that the Stored Communications Act did not authorize extraterritorial application, and that the government could obtain the data through the mutual legal assistance process instead. This case has important implications for cross-border data transfers and the extraterritorial reach of U.S. law. *Carpenter v. United States* (2018): in this case, the US Supreme Court held that the government must obtain a warrant before accessing historical cell phone location data from a third-party provider. *Sony BMG Music Entertainment v. Tenenbaum* (2009): in this case, the defendant was found liable for copyright infringement for sharing music files on peer-to-peer networks. *Google LLC v. Oracle America Inc.* (2021): in this case, the US Supreme Court held that Google's use of certain Java APIs in its Android operating system constituted fair use under copyright law.

These cases illustrate how technology is being used to improve access to justice and enhance the effectiveness of the legal system. Most importantly, it highlights the fact that without a thorough knowledge of technology, legal practitioners of today cannot be effective in the courtroom.

I encourage you to explore the articles in this Journal and engage with the ideas presented here. I believe that the International University of East Africa's newly launched African Journal of Legal Issues in Technology and Innovation will serve as a valuable resource for anyone interested in the future of law and the role that technology is playing in shaping it.

Prof. Emeka Akaezuwa

VICE CHANCELLOR
INTERNATIONAL UNIVERSITY OF EAST AFRICA

We welcome you to the inaugural issue of the African Journal on Legal Issues in Technology and Innovation (AJLITI), a peer-reviewed publication of the International University of East Africa (IUEA). This Journal is a trailblazer in East Africa and encompasses scholarship relevant to our times – best referred to as the "digital age" or the "Fourth Industrial Revolution".

We begin by expressing our utmost gratitude to the authors who have contributed their articles to this Journal, without whom this project would neither have taken off nor come to life.

In this exciting inaugural issue, we have a wide range of articles on various topics intersecting between technology, innovation and the law, summaries of which we now delve into.

Irene Eyogyiire starts us off with decentralised finance (De-Fi) and explores how it can be leveraged in the capital markets space with its inherent qualities of visibility of trading activity, non-intermediation and transaction efficiency. She accepts that De-Fi comes with its risks but contends that its advantages outweigh those risks so that it should be given a chance to contribute to the development of the nascent capital markets sector in Uganda.

Uche Anyamele dives into the novel area of Central Bank Digital Currencies (CBDCs) in the East African Community (EAC). According to Anyamele, the EAC is steadily progressing towards a Monetary Union with a goal to introduce a single currency. Indeed, the EAC Monetary Institute is already in the works, and some Partner States are already discussing CBDCs at the regional level. As such, she argues, there is justification for a comprehensive legal framework to support CBDCs. Using comparative examples from other jurisdictions, Anyamele recommends mechanisms for designing a suitable CBDC policy and legal framework for the EAC.

Chidochashe Ncube explains how blockchain technology can be used to facilitate intra-African trade. Ncube argues that blockchain technology can deliver the full operationalization of the African Continental Free Trade Area (AfCFTA). A single window, which traditionally is a single-entry point that allows traders to access and submit documents electronically, can benefit incredibly from the features of the blockchain system. Ncube demonstrates that the core function of a single window is to expedite and simplify information flows between traders and government agencies, bringing meaningful gains in time, security and efficiency for all parties involved in cross-border trade. Blockchain technology, she suggests, ensures trustworthiness, security of data as well as consensus among participants in the network, limiting fraud as transactions are verified and tracked.

Paul Mukiibi explores the regulation of electronic signatures in Uganda. He maintains that although it has been over ten years since the enactment of the Electronic Signatures Act in Uganda – which was enacted to regulate the use of electronic signatures – there are still major challenges as far as the full implementation of this law is concerned, particularly in civil proceedings. Drawing on comparative examples globally, Mukiibi highlights the need for the harmonization of this law with other existing laws, advocates for the establishment of the relevant technological infrastructure for electronic transactions and stresses the need to build stakeholder capacity to ensure that the law achieves its full potential.

Godfrey Ayeranga assesses the impact of video conferencing technology on prisoners' rights to a fair trial in Uganda. Ayeranga notes that although video conferencing for prisoners was adopted in Uganda to mitigate against the spread of COVID-19 amongst prisoners and court users, its continued use in criminal proceedings presents significant challenges that affect the credibility of the trial process and limit the prisoner's right to a fair trial – ranging from poor internet connections that affect the quality of proceedings, to lawyers and Judges not being able to make out the body language of the accused and witnesses, and prisoners not being able to consult their lawyers in real time during the trial, among others. However, Ayeranga helpfully recommends how video conferencing technology can be improved to ensure a fair hearing and justice delivery for prisoners.

Mujib Jimoh illustrates the interaction between surveillance technology and human rights. He thoroughly interrogates this topic in the context of our modern day and age where surveillance technology is susceptible to abuse by governments. In so doing, Jimoh provides a critical analysis of governments' rationale for surveillance and measures it against the human rights guaranteed by the African Charter on Human and Peoples' Rights as well as other regional and national instruments that make up the African human rights legal system. Jimoh concludes by advocating for a binding legal instrument regarding digital surveillance in Africa.

Augustine Ochieng provides an account of how the digital economy helped the EAC stave off the debilitating effects of COVID-19. Ochieng, for example, discusses the significance of mobile money during the pandemic, as it had already taken root in the region prior to the pandemic. He also asserts that e-commerce had struggled for a long time but received a major shot in the arm during the pandemic. Ochieng advocates for the Partner States to leverage on the consumer adoption of these technologies to enhance their economies in the post-COVID-19 era, through robust and comprehensive legal frameworks that ensure fiscal and regulatory compliance of non-resident entities. Ochieng acknowledges the challenges in attaining this goal and provides recommendations on how they can be resolved.

Peter Keya renders an appraisal of the use of technology in the Kenyan Presidential election of 2017 – the first time that technology was used in a general election in Kenya. In 2017, the Elections Act in Keya was amended to establish an integrated, biometrical electoral system – a system that was meant to be "simple, accurate, verifiable, secure, accountable and transparent." Keya interrogates whether the technology used in subsequent Presidential elections meets that standard. He concludes by suggesting recommendations to address the ever-present "technology question" in future Kenyan Presidential elections.

Joshua Kingdom takes us to the Metaverse and Artificial Intelligence (AI). He discusses the challenges that are likely to come with this paradigm shift in our way of life and calls for regulators and stakeholders to be alive to this reality. Kingdom argues that regulators ought to be proactive, vigilant and teachable in their quest for regulatory answers to the novel questions presented by the advent of the Metaverse and AI. Hinging on the testimony of Frances Haugen – a former Facebook executive turned whistleblower – Kingdom highlights the potential unconscionable aspects of emerging technologies and identifies the major angles that regulators should consider.

Nasser Konde offers a critique on the mechanisms used for surveillance in Uganda, including digital surveillance of motor vehicles. He analyses their lawfulness in the context of Ugandan law, and offers a detailed comparative analysis with Southern Africa, Europe, Asia and the United States of America.

Konde discusses the human rights implications of surveillance in the context of Uganda's Constitution, while providing recommendations for the lawful and proportionate approaches to achieving the objectives of surveillance.

Lastly, Sanatu Mustapha Alidu, Samuel Oppong Abebrese and Amina Moro discuss plant breeders' rights. They posit that plant variety protection systems were established by African countries to, among other things, allow farmers to access a wide range of improved varieties and ensure food security. However, those systems have now come under significant resistance on the primary ground that they are unsuitable for Africa. Alidu, Abebrese and Moro provide regulatory case studies of Ghana, Uganda and Kenya while striking a balancing act between the arguments for and against this resistance.

Once again, we would like to express our sincere gratitude to the authors and acknowledge their patience plus cooperation during the publication process.

We also warmly applaud the Vice Chancellor of IUEA for his constant support for the initiatives of the Faculty of Law as well as his unwavering dedication to the advancement and use of technology in the teaching, study and application of law. In similar spirit, we acknowledge the support received from the various offices at IUEA – including the Resident Director, University Secretary and Marketing Department – for facilitating the publication of this Journal and the organization of the conference from which the Journal arose, i.e., the 2nd Annual IUEA Tech Law Summit in December 2022. We look forward with great excitement to the 3rd Annual IUEA Tech Law Summit in December 2023, and to the subsequent publication of our next issue arising out of that conference.

We now welcome readers to indulge and enjoy the amazing scholarship in this Journal, which should go a long way in informing policy in Africa and beyond.

Emmanuel Sebijjo Ssemmanda
Ivan Ojakol

EDITORS-IN-CHIEF
AFRICAN JOURNAL OF LEGAL ISSUES IN TECHNOLOGY AND INNOVATION
INTERNATIONAL UNIVERSITY OF EAST AFRICA, FACULTY OF LAW

EASE THE REGULATORY SCEPTICISM: WE DO NOT HAVE TO THROW THE DE-FI BABY OUT WITH THE BATH WATER

Irene Eyogyiire[*]

ABSTRACT

This paper considers the key characteristics of distributed ledger financial technological innovations and argues that instead of blocking their use and development, Uganda can take advantage of the developments in decentralised finance (De-Fi) to drive the growth of capital markets. An observation of the interactions between regulators and players/innovators in the De-Fi technology space shows a high level of scepticism towards crypto-currencies and analogous schemes. While this wariness is not unfounded, there are certain aspects of De-Fi that can be imitated (with modification) for the achievement of the Capital Markets Authority's overarching objective to wit promotion of the development of capital markets in Uganda.

The paper draws parallels between existing products/concepts within Uganda's capital markets law (including asset backed securities, commercial paper, corporate debenture issuances, etc.) and innovations within the De-Fi space to demonstrate the way those innovations can be customized for targeted purposes. Considering the key advantages of public ledger technology, including visibility of trading activity, non-intermediation and transaction efficiency, adoption of similar ideas in the capital market space could likely drive growth. The paper asserts that despite the risks associated with these technological applications, they are worth exploring to spur growth within the nascent/under-developed capital markets. These under-developed capital markets could ride the DeFi-wave and capture the idle but available capital waiting for worthy ventures in which to invest.

The paper is divided into four sections: Section I is a brief overview of De-Fi and the current usage in the fin-tech space. Section II demonstrates that the salient features of De-FI are reminiscent of certain capital markets products. Section 3 proposes ways in which the mechanisms underlying DeFi can be adopted in a capital markets context while addressing their inherent risks. Section 4 is a conclusion of the discussions in the paper.

[*] Irene Eyogyiire is a Lecturer of Law at the International University of East Africa and Partner at Bytelex Advocates in charge of the Finance, Tax and Energy Department. She holds a Master of Science (Msc) in Law and Accounting from the London School of Economics; a Bachelor of Laws (LLB) from Makerere University, Kampala and a Post-Graduate Diploma in Legal Practice (PGDip. L.P) from the Law Development Centre.

INTRODUCTION

In recent years, the developments in the financial services sector especially the uptake of digital representations of money and other virtual representations of value have been at the centre of numerous discussions in financial services regulation. Central banks and securities regulators have been confronted with the urgent need to define the new players in the financial services sector. Financial technology innovations have re-defined the landscape in different areas of financial services ranging from payments and remittances, credit accommodation, capital raising from the public, credit scoring, and investment advisory. The subject of this article is the financial technological innovation embodied in distributed ledger technology.

The pioneer application of Distributed Ledger Technology (DLT) was the infamous virtual currency, Bitcoin.[1] The growing use of this virtual currency was looked upon warily by regulators globally, with express criminalisation in certain countries. This was largely since virtual currencies were proposing an alternative financial system that would run parallel to the existing centralised and intermediated system without the safeguards that had been built to ensure stability of the financial system.

Against the backdrop of this sceptical view taken of DLT based digital assets, this paper will put forward a suggestion for a non-currency application of DLT. The thesis of this paper is that distributed ledger technology (DLT) is the baby that should not be thrown out with the murky bath water of digital coins and assets. DLT could potentially be applied with modifications to achieve efficiency in the financial services sector apart from usage in virtual currencies. Drawing from earlier observations that DLT innovation would trigger a new way of thinking within the financial services sector[2], we explore the potential application of DLT in securities and the legal issues that would arise. This paper considers the overarching objectives of the creators of DLT, the features and other efficiencies promised by DLT to suggest a non-currency application of DLT in capital markets.

Regulation can influence the trend of development of technology and harness it for the fulfilment of overall sector objectives. With a bespoke application of DLT, regulators and market participants can collaborate to design a platform that will drive the growth of investment by the public in capital market instruments. In the existence of a larger enabling platform, smaller financial technology firms would piggyback on the infrastructural backbone to establish small applications for trading and wallet hosting. Riding on network effects and the virtuous cycle of lower costs, the entire market would reap the benefits of having the more users utilizing the platform and consequently the increased efficiency of transactions.

Various policy makers have adopted a technology neutral approach to regulation

[1]Angelos Deliverias, 'Distributed Ledger Technology and Financial Markets', (2016) European Parliamentary Research Service, PE 593.565. Distributed Ledger Technology is used in this paper to refer to technologies that enable creation of distributed databases across multiple sites, countries or institutions, which are typically accessible by anyone, that keep records of transactions. These distributed ledger technologies include Blockchain technology and similar methodologies.

[2] Robleh Ali, John Barrdear, Roger Clews and James Southgate, 'The Economics of Digital Currencies', (September 2014), Bank of England Quarterly bulletin, predicted that in the future DLT could be thought of as the internet of finance stretching its application beyond currency and payments into other areas of finance where records are stored digitally.

of the new entrants focussing on the nature of activity. This approach, also referred to as same activity same regulation, not only creates a level playing field for all actors within a particular sector but also incentivises the adoption of technology in service delivery.

This policy approach has however not proved suitable for regulation virtual asset service providers because of the certain characteristics that are crypto-asset specific. These characteristics explain why crypto assets have largely remained out of the reach of regulators. First and foremost, the decentralised nature of the De-Fi technology makes it difficult to identify the entity/player that should be responsible for compliance with regulatory obligations. Secondly, by their nature the first-generation crypto assets like Bitcoin and Ethereum do not exhibit any characteristics of specified regulated instruments.

The inability to comfortably bring something within one's regulatory purview understandably makes regulators jittery especially where there are clear risks associated with a particular business activity. Regulatory panic is justified where control of cross border financial flows, whether illicit or not, cannot be monitored effectively. Similarly, where there is public outcry of 'crypto-linked' scams the pressure to outlaw all similar activities is high.[3] Privacy or anonymity of DLT transactions poses a challenge to regulatory control of money laundering and terrorism financing.[4] Not forgetting the consumer protection challenges arising from deliberate misinformation or very scanty disclosures by unknown crypto-asset issuers.

Notwithstanding, these well-founded regulatory concerns, one can argue that the proliferation of crypto-asset use within East Africa is partly due to the ingenuity that underlies the idea of distributed ledger-based assets and the search for alternative investment opportunities. We take a simplistic view of the working of the technology to argue that instead of banning all things that bear resemblance to crypto assets, an alternative/replacement good can be provided to sate the public appetite for new forms of investment opportunities.

Before we dive into the discussion on the possible application of DLTs in the capital markets arena to increase public participation, we must set out the definition of key terms that will be used in this paper.

1. TAXONOMY

Distributed Ledger Technology means a secure database or ledger replicated across multiple sites, countries or institutions either with or without a central controller.[5] The essence of DLT is to record in a digital ledger every transaction made on the network in identical copies of a ledger which are replicated (distributed) among users.[6] Records are stored one after another in a continuous

[3] Bank of Uganda (2017), Warning to the Public About 'One Coin Digital Money' Operations in Uganda, Press Release in which Bank of Uganda warned the public against investing in One-coin, Bitcoin, Ripple, Peercoin, Namecoin, Dogecoin, Litecoin, Bytecoin, Primecoin, Blackcoin or any other forms of Digital Currency.

[4] European Central Bank (2019), 'Crypto assets: Implications for Financial Stability, Monetary Policy, and Payments and Market Infrastructures', Occasional Paper Series No. 223/2019.

[5] Deliverias (n 1). See also, Leon Perlman, Security Aspects of Distributed Ledger Technology, (2020) International Technology Union - Security, Infrastructure and Trust Working Group at p.13.

[6] Ibid.

ledger. This technology enables tracking of who owns a financial, physical or electronic (digital) asset.

DLT-based asset or token (also referred to as crypto-asset/token) is discussed in this paper to broadly refer to any privately issued digital asset that depends on cryptography and distributed ledger technology for issuance and recordkeeping.[7] In general, this definition can be extended to three broad categorisation of DLT-based assets including first generation, second generation and other DLT based tokens.

First generation DLT-based assets (also called crypto assets) refer to digital assets that represent a new unit of account/currency; are not issued by an identifiable person or authority thereby not representing a claim on an issuer; with no intrinsic value and are not backed by any other assets and having their price driven by the activity of their holders and users.[8] These include Bitcoin, Ethereum and similar coins that are self-contained not carrying any ancillary or secondary promise to lend to their value or existence.[9]

Second generation crypto assets including stable coins such as United States Dollar Tether (USDT) whose aim is to maintain a stable value relative to a specific asset.[10] As such their value is linked to a specified fiat currency, an asset or pool of assets. Depending on their structure and usage, they could fall under payments, securities or even require bespoke regulations.[11]

This paper shall focus on the species of DLT-based assets/tokens that can be characterised as securities because they represent an ownership, debt or other claim on the issuers. These can be fitted within the definition of existing financial instruments or securities including shares, debt securities, units in a collective investment scheme, e-money tokens and other regulated tokens.

2. THE ATTRACTIVE FEATURES OF DISTRIBUTED LEDGER TECHNOLOGY

The positive and essentially seductive propositions of DLT is that it is touted as being able to achieve the following: decentralisation; dis-intermediation; peer to peer transacting; resolve the double-spending problem associated with electronic communications; and enhancement of transaction security.

Dis-intermediation. Dis-intermediation is the claim that use of DLT based applications would enable the elimination of so called 'trusted' intermediaries who had become custodians of the financial services system. The primary disruptive characteristic of DLT is that the database is decentralised and not dependent on a centralised authority to store, facilitate and authorise transactions.[12] This particular characteristic has been consistently championed as a justification for the initial mass adoption of DLT based virtual currencies (crypto-currencies).[13] Many

[7] Parma Bains, Dimitris Drakopoulos, Federico Grinberg, Evan Papageorgiou, Nobuyasu Sugimoto, 'Global Financial Stability Report - Online Annex 2.1 Technical Note' (2021) International Monetary Fund.

[8] See Parma Bains et al (2021) supra n 7. European Central Bank, 'Crypto assets: Implications for Financial Stability, Monetary Policy, Payments and Market Infrastructures', supra n 4 at p.3.

[9] Edmund Schuster, 'Cloud Crypto Land', (2019) LSE Law, Society and Economy Working Papers 17/2019 accessed at https://ssrn.com/abstract=3476678 on 10th July 2022.

[10] Parma Bains et al (2021) supra n 7.

[11] Parma Bains et al (2021) supra n 7.

[12] Leon Perlman (2020), supra n 5.

[13] Ali Robleh et al (2014) supra n 2 for the assertion that the foundational motivations of the design

pioneering proponents argued that a financial system based on DLT would not suffer from the moral hazard that plagues the traditional financial system.

Decentralisation means that DLT platforms bring with them the promise of scalability because their usage is not limited by physical presence. Crypto assets can be transferred across jurisdictions without the need for physical infrastructure other than the internet.[14] This characteristic implies that regardless of one's physical location they can acquire crypto assets, they have access to their account and real-time information on the market price of their assets. This is in fact the major reason underlying the frequent use of crypto assets for execution of cross-border money remittance transactions.[15]

Peer to peer transacting. The design of the infrastructure allows person to person transactions without the involvement of a central authority to confirm the validity of the transaction. The network users. Distributed ledger technology can attribute an asset to each individual user and the holder is able to transact in the asset without the need for an intermediary.[16] The technology is designed to enable any holder to directly transfer their assets to another person and the new holder of the assets would be treated as owner of the assets.[17]

Double-spending problem. DLT is also lauded for resolving the double-spending problem which is a feature of all electronic communications. Edmund Schuster explains that historically the inability to objectively or chronologically order two messages posed a seemingly insurmountable problem for the creation of a protocol allowing for peer-to-peer transfers of digital assets.[18] The mainstream financial system depends on the existence of a trusted intermediary to order and authorize transactions between parties after confirming balances and existence of assets.[19] In a DLT based structure, all participants have access to information relating to transactions affecting any particular coin and all accounts are regularly and automatically consolidated through the internet.[20] By enabling a network wide consensus on the ownership of digital asset and transaction history affecting any particular asset, DLT eliminates the risk that any given coin can be spent more than once or asset transferred by a holder to more than one person.

The security capabilities of DLT including an immutable ledger, cryptographic signatures and keys offer a level of comfort against the fear that public access to the ledger will compromise the safety of one's asset holdings. DLT uses cryptography to securely store data, cryptographic signatures and keys to allow access only to authorized users.[21] The technology also creates an immutable database, which means information, once stored, cannot be deleted and any updates are permanently recorded for posterity.

---

for bitcoin was the desire to avoid any centralised control (of either the money supply or the payment system) and to minimise the trust that participants need to place in any third party.

[14]Phillip Paech, 'Securities Intermediation and the Blockchain – An Inevitable Choice Between Liquidity and Legal Certainty', (2016) Uniform Law Review 21 (4).

[15] Dong He, Ross B. Lecklow, Vikram Haksah, Tomasso Mancini Griffoli, Nigel Jenkinson, Mikari Kashima, Tanai Khiaonarong, Celia Rochon, Herve Tourpe, 'Fintech and Financial Services: Initial Considerations', (2017) International Monetary Fund Staff Discussion Notes (SDN) at p.23.

[16] Phillip Paech (2016), supra n 14.

[17] Parma Bains et al (2021) supra n 7.

[18] Edmund Schuster (2019), supra n 9.

[19] Edmund Schuster (2019) supra n 9.

[20] Phillip Paech (2016) supra n 14.

[21] Leon Perlman (2020) supra n 5.

The ideals discussed above may not have been achieved in their purest form due to operational realities, but they still suggest use-cases of DLT infrastructure that can augment the existing financial services infrastructure.

3. THE POINT OF INTERSECTION: DLT - THE CHANNEL TO SECURITIES MARKET UTOPIA

In a report published by the Capital Markets Authority relating to the performance of Collective Investment Schemes (CISs), poor savings and investment culture was cited as one of the hindrances to investment in CISs. In recent years, there has been a marked growth in individual savings in collective arrangements such as investment clubs and savings and cooperatives. This means that the public is alive to the advantages of pooling of capital for investment, but they have not been enticed enough to invest in traded securities.

An observation of the capital markets in Uganda shows that stirring up the public to view securities as a viable investment option takes much more than putting in place the legal and regulatory framework for issuance of the securities and supervision of sector players. The role of the regulator goes beyond public sensitization and driving engagement and extends to supporting innovation and facilitating any endeavours that would resolve existing inefficiencies/shortcomings within the market.

Shortcomings are deemed to exist within the financial services where sector improvements can be made to attributes of services that would induce a jump in demand evidenced by users' willingness to pay more for the new service, or consume more of it at unchanged prices.[22] DLT has the potential to offer solutions that could resolve the existing shortcomings and any DLT-inspired solution would be best implemented with support of the regulator.

Without a doubt, the saving (and investing) public is always searching for investment opportunities and are even willing to place a bet on any new fad which promises a return. In a recent Kenya High Court decision Wiseman Talent Ventures v. Capital Markets Authority (2019)[23], the issuer of a digital asset referred to as 'KeniCoin' protested the injunctive intervention of the Capital Markets Authority of Kenya (CMA-K) in their business. Prior to the intervention of the CMA-K, some members of the public had already invested in KeniCoin despite the absence of key information such as the structure and processes of the business and viability of the KeniCoin. The court ruled that KeniCoin exhibited the characteristics of a security and as such the advertising and trading of KeniCoin fell within the regulatory ambit of CMA-K. Such occurrences provide evidence that the public has embraced the idea of digital representations of value even during outright warnings from regulatory authorities to the public to deal cautiously with ambiguous investment opportunities in the crypto sphere.

Inferences can also be drawn from recent press releases and actions of the Central Bank of Uganda that the volume of crypto-asset transactions involving local persons (or within Uganda) have hit the significance threshold.[24] While those

[22] Dong He et al (2017) supra n 15.

[23] High Court of Kenya Civil Suit No. 08 of 2019.

[24] Bank of Uganda (2022), Circular dated 29th April 2022 prohibiting licensed payment service providers under the National Payments Systems Act from providing cash out options for persons dealing in crypto currencies. Johnstone Kpilaaka, 'Bank of Uganda to allow crypto models on its

figures showing trading activity in crypto assets within Uganda may arguably be attributable to payments or cross-border remittances, one can argue that they are an indicator that certain persons are holders (whether speculative or not) who view those crypto assets as an investment instrument. If the investing public is willing to invest in crypto assets in respect of which information is scant, wouldn't enhancement of the distribution channels for legitimate securities result in development of a vibrant securities market?

One of the overarching objectives of the Capital Markets Authority (CMA) is to have a vibrant securities market with the public buying and selling securities. An online securities trading platform imitating a DLT-based platforms is a possible route to achievement of this objective. This is because of those attributes of a DLT based system that can be leveraged to capture the evident investor interest and effectively attract the available and un-deployed funds into worthy investments.

Capital markets are a modern-day financing option that was developed out of the idea that entities can raise investment capital from the public instead of an individual financier. The financial need is broken up into up smaller digestible portions and the invitation extended to many investors. To achieve this, securities take the form of standardised fungible units of finance thereby allowing financiers (investors) to participate in the investment to the extent of their risk appetite.[25] Existing classes of securities (shares, debt securities and other units) have already been structured as standardised fungible units and are represented in electronic ledgers.[26] For these securities, a DLT-based platform would not only provide an electronic record of each individual investor's claim against the issuer but a trading platform where they can interact with other holders and potential buyers.

In addition to easing first time investing, a lively secondary market for such securities would emerge because the security tokens would be fungible and transferable on a peer-to-peer basis. Micheler advances the argument that creation of transferable fungible units contributes a great deal to achievement of a vibrant securities market as it enables pricing of securities by market participants and provides investors with liquidity should they desire to exit the investment.[27] This design of the securities coupled with the twin efficiencies of accessibility and convenience of the platform may be the wind required to fan the flames of a largely dormant secondary market for securities.

A DLT platform and the ecosystem of players that would emerge in the existence of such a platform would result in a more efficient matching of buyers and sellers of securities. This would be advantageous for entrepreneurs looking for capital, new investors, and exiting investors. Dong He et al highlight that intermediaries exist within financial markets because of market imperfections, one

---

Regulatory Sandbox' (2022) accessed online at https://www.benjamindada.com/bank-of-uganda-crypto-regulatory-sandbox/ on 7th August 2022 quotes CoinTelegraph statistics *'…between 2020 and 2021, crypto use in Africa increased by nearly 1,200% and nearly 2% of Ugandans use crypto.*'

[25]Eva Micheler, Legal Nature of Securities: Inspirations from Comparative Law. (2020) in Gullifer, Louise and Payne, Jennifer, (eds.) Intermediated Securities: Legal Problems and Practical Issues. Hart Publishing, Oxford, UK, pp. 131-148. ISBN 9781849460132 electronic copy available at: https://ssrn.com/abstarct=1481427 accessed on 7th June 2022.

[26] Organisation for Economic Cooperation and Development, 'Regulatory Approaches to Tokenised Assets', (2021) OECD Blockchain Policy Series accessed at https://www.oecd.org/finance/Regulatory-Approaches-to-the-Tokenisation-of-Assets.htm on 9th June 2022

[27] Eva Micheler (2010) supra n 25.

of which is the matching asymmetries.[28] Intermediaries resolve matching asymmetries by facilitating the matching of those who need capital and with savers who are providers of capital.[29] DLT would substantially alter the structure of the financial markets by reducing the role of intermediaries and enabling holders to directly offer their securities holdings for sale to willing buyers.

Liquidity resulting from the vibrant secondary market would also raise investor interest in the securities. Phillip Paech posits that the use of DLT may provide a better way to achieve the aims of liquidity due to the peer-to-peer trading feature.[30] Investors will show a preference in investing in any type of asset that offers a certain level of flexibility at the point when they desire to liquidate. The attractiveness of certain kinds of securities has, in certain instances, been associated with the existence of a mechanism for discontinuation one's investment at any stage.[31] Therefore an investment option that gives financier an element of flexibility has an advantage over an illiquid investment.

Furthermore, a liquid secondary market would also ease the pressure imposed on collective investment schemes when handling and/or managing investor exits and capital redemption demands. To stem the unprecedented exit of investors, collective investment arrangements often devise disguised lock-in clauses intended to dis-incentivise the exit of members from the investment scheme. Existing scheme members are reluctant to exit the scheme where there is a loss suffered by the member who opts to exit from the investment company/club. In Tushabomwe John v. Western Young Investors Association Limited[32], the High Court of Uganda adjudicated a dispute involving an existing member who objected to the pay-out made to him by the club operator upon his exit. In the balances, the court found that although the clause negatively altered his entitlement it was in the best interests of the scheme and had to be given effect. Such a result has the potential to discourage potential investors in any collective investment arrangement. Instead of forcing a redemption out of the capital fund of the issuer, the market should provide the investor with a cash out option thereby making this form of asset an attractive investment option.

Decentralisation of the ledger opens the door for diaspora investors. Many migrant labourers would exploit this cross-border investment opportunity due to the certainty and assurance that their monies have not been diverted by self-seeking middlemen (or relatives). These monies invested in DLT-securities can then easily be redeemed when the immigrant workers are back home without the worry of having to make large cash transfers.

In theory, individual holding of securities on a DLT-based platform could transform those securities into acceptable collateral in credit transactions involving third party credit providers. Rather than having a dormant stock of securities while you wait hopefully for the issuer to declare a dividend or other distribution, the electronic securities can be pledged in a short-term financing transaction.

---

[28] Dong He (2017), supra n 15.
[29] Dong et al (2017), supra n 15.
[30] Phillip Paech, Securities (2016), supra n 14.
[31] Jens Burchadt, Ulrich Hommel, Dzidziso Samuel Kamuriwo and Carolina Billiteri,'Venture Capital Contracting in Theory and Practice, Implications for Entrepreneurship Research' (2016) Entrepreneurship Theory and Practice.
[32] Tushabomwe John v. Western Young Investors Association Limited High Court (Commercial Court) Civil Suit No. 1032 of 2022.

The picture painted in this section is purposefully rosy and glosses over the many limitations associated with the DLT. Pertinent questions relate to internet access and availability of devices that can support use of the technology. Given the current level of internet penetration, a DLT based solution may not be the appropriate distribution channel to drive consumption by the wider population. Despite these obvious failings, the promises of convenience and accessibility are enough to entice a thoughtful consideration of the technology.

The preceding discussion attempts to demonstrate how DLT can indeed contribute to improvement of the operational environment including the design of issued securities, registration and holding of securities as well as their transfer between parties. With these factors working together to facilitate the development of the securities market, the next consideration is what tweaks need to be made to the oversight legal and regulatory framework to integrate DLT.

4. REGULATION: THE WHEEL IS NOT BEING REINVENTED, ATLEAST NOT THE ENTIRE WHEEL

The final question then remains, what would a sound financial law and regulatory framework for DLT-based securities look like. In addition to the existing regulation aimed at controlling money laundering and terrorist financing by Virtual Asset Service Providers[33], the key aspects that would have to be addressed include market integrity, consumer and investor protection, legal certainty – enforceability of rights in those securities, security of assets, insolvency of issuers and holders.

The legal and regulatory framework necessary to support the adoption of a DLT based securities trading platform shall not be developed from scratch. The bulk of the work will be to provide for regulation of new risks that emerge because of deployment of DLT and having digital representations of elements already provided for within the existing law. It is important to ensure that the safeguards present in traditional financial markets will equally apply in DLT based systems. Examples can be drawn from certain jurisdictions that have acknowledged existence of crypto-securities and taken steps to define their place within the regulatory framework. Their approaches are worth considering and can inform the development of an appropriate regulatory framework in Uganda.

4.1. Regulatory Approach taken in Crypto-friendly Jurisdictions

Instead of ignoring the budding ecosystem, certain jurisdictions have adopted a stance that accommodates the developments in the crypto sphere. Considering the fact that existing regulatory frameworks were built for a centralized financial system, the regulation must adjust to the decentralized nature of financial technologies. With the mind that regulation should not stifle innovation but build trust[34], these jurisdictions have developed frameworks that embrace the new

[33] The Anti-Money Laundering Act, 2013. The Anti-Money Laundering (Amendment of Second Schedule) Instrument, Statutory Instrument No. 136 of 2020 designate Virtual Asset Service Providers as accountable persons who must comply with certain reporting requirements.

[34] Cristina Cuervo, Anastasiia Morozova, Nobuyasu Sugimoto, Regulation of Crypto Assets, International Monetary Fund, Fin- tech Note 19/03, (2019).

technology while putting in place the appropriate safeguards. In this section, we set out a summary of the regulatory approach taken by two 'crypto-friendly' jurisdictions viz the United Kingdom and Nigeria.

United Kingdom

Against the backdrop of various reports and commentaries regarding regulation of crypto assets, some countries opted to develop bespoke regulatory regimes for crypto assets.[35] The overall perception was that the absence of a clear regulatory framework was one of the main impediments to growth of the digital capital markets as an alternative source of finance for small and medium enterprises.

The United Kingdom has not enacted bespoke laws or regulations to govern issuance of crypto assets but has taken an overall approach that can be summarised along two principles: 'substance over form' and 'technology neutrality'. The 'substance over form' approach ensures that the essential characteristics of the token, not the label assigned by the issuer, are given weight when characterising the token. Technology neutrality means the use of a specific kind of technology does not impact on kind of regulatory permissions that must be obtained by the entity carrying on the regulated activity. As such in addition to putting measures in place to comply with the applicable regulation, the entity must take precautions to address the peculiar operational risks associated with its type of technology.

Guided by these principles, the Financial Conduct Authority issued Guidance on Crypto assets[36] with the primary objectives of reducing legal uncertainty and creating an environment in which firms are stimulated to develop legitimate crypto-asset activities and business models.

Classification. The FCA Guidance provides clarity to market participants on the type of crypto assets that fall within their regulatory remit, the resulting compliance obligations and regulatory protections to consumers. The FCA guidance categorised crypto assets in three (3) broad categories including: Unregulated tokens, e-money tokens and security tokens. The latter two categories are subject to regulation by the FCA.

Unregulated tokens are tokens that are outside the financial regulatory perimeter because they do not fit within the existing scope of regulated activities under the FSMA regulatory framework.[37] The Guidance gives examples of unregulated tokens to include exchange tokens and utility tokens. Exchange tokens are defined as tokens that are not issued or backed by any central authority and are intended and designed to be used as a means of exchange. They tend to be a decentralised tool for buying and selling goods and services without traditional intermediaries. Exchange tokens are used in a way like traditional fiat currency but have no central issuer backing up their value. Examples include Bitcoin and Ethereum.

On the other hand, utility tokens are defined as those tokens that provide consumers with access to a current or prospective product or service and often grant rights like pre-payment vouchers.

E-money tokens which by virtue of their characteristics satisfy the definition of

[35]Agata Ferreira and Philip Sandner, EU Search for regulatory answers to crypto assets and their place in the financial markets' infrastructure, Computer Law and Security Review 43 (2021) 105632

[36] Financial Conduct Authority (FCA), Guidance on Crypto assets: Feedback and Final Guidance to CP 19/3, Policy Statement PS19/22 (2019)

[37] FCA Guidance on Crypto assets supra n 36, paragraph 34 defines unregulated tokens as those tokens that do not provide rights or obligations akin to specified investments (like shares, debt securities and e-money).

electronic money as defined by Electronic Money Regulations, 2011 ('EMR')[38] are subject to that regulatory regime. Some fiat-backed stable coins can therefore be categorised as e-money tokens where their value is directly linked to the value of a specified fiat currency and the issuer holds a reserve of the fiat currency to guarantee the value of the tokens.

Security tokens are defined as those tokens with specific characteristics that mean they provide rights and obligations akin to specified investments, such as shares or debt instruments. Specified investments are those set out in the Regulated Activities Order (RAO), 2001[39] and they include those investments that fit the definition of financial instruments or transferable securities under the Markets in Financial Instruments Directive II ('MIFID II').

Where crypto assets satisfy the requirements then they are brought under the general prohibition under Section 19 of the Financial Services and Markets Act, 2000 ('FSMA') which prohibits persons from conducting any regulated activity without the necessary authorisation. The FCA Guidance further draws clear lines to guide sector players in determining whether a crypto-asset or token would be a security token and as such subject to regulation. The FCA Guidance highlights some of the factors that are indicative of a token being a security token, including the following:

- "the contractual rights and obligations the token-holder has by virtue of holding or owning that crypto-asset
- any contractual entitlement to profit-share (like dividends), revenues, or other payment or benefit of any kind
- any contractual entitlement to ownership in, or control of, the token issuer or other relevant person (like voting rights)
- the language used in relevant documentation, like token 'whitepapers', that suggests the tokens are intended to function as an investment, although it should be noted that the substance of the token (and not the label used) will determine whether an instrument is a specified investment
- whether the token is transferable and tradeable on cryptoasset exchanges or any other type of exchange or market
- a direct flow of payment from the issuer or other relevant party to token holders may be one of the indicators that the token is a security, although an indirect flow of payment (for instance through profits or payments derived exclusively from the secondary market) would not necessarily indicate the contrary."[40]

In line with the guidance issued by the FCA, any person issuing and/or dealing in crypto tokens that satisfy the characteristics of transferable securities[41] is subject to regulation under the Financial Services Markets Act (FSMA), 2000 and the

[38] Financial Services and Markets Act (Electronic Money) Regulations, No. 99 of 2011, regulation 2 defines electronic money to mean electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer which— (a) is issued on receipt of funds for the purpose of making payment transactions; (b) is accepted by a person other than the electronic money issuer.

[39] Financial Services and Markets (Regulated Activities Order), 2001, Articles 76 and 77

[40] FCA Guidance on Crypto assets, supra n 36, p 34.

[41] European Union, Directive No. 2014/65/EU of the European Parliament and of the Council on Markets In Financial Instruments Directive II (MIFID II) .

Financial Services (Regulated Activities Order), 2001.

4.1.1. Nigeria

Nigeria, which is one of the largest markets from crypto assets in Africa, has issued bespoke Rules on Issuance, Offering Platforms and Custody of Digital Assets ('the Rules').[42] The Rules are directly applicable to all issuers seeking to raise capital through digital asset offerings.

Classification. The Rules categorise digital assets into discrete categories including virtual assets and other digital assets that are subject to regulation by virtue of what they represent. Virtual assets are defined as digital representations of value that can be traded and can be used for payment or investment purposes which are not a representation of fiat currencies, securities and other financial assets. The Rules make specific provision for the regulatory framework that applies to virtual assets which do not satisfy the definition of any financial asset.

On the other hand, Digital assets are defined to mean digital tokens that represent assets such as a debt or equity claim on the issuer.[43] This definition of digital assets is extended to capture fiat or e-money tokens and security tokens. Such tokens are subject to regulation under existing laws in Nigeria.

The Rules specifically state that any offering of digital tokens that are considered securities using distributed ledger technology (DLT) is subject to regulation.[44] Whether digital assets qualify as securities is determined in accordance with the definitions in the existing applicable laws including Investments and Securities Act, 2007 and Securities and Exchange Commission Rules and Regulations.

Regulated persons. The persons who are subject to registration and approval under the Rules include:

Any promoters, entities or businesses intending to offer a digital asset/token that constitutes a security within Nigeria or targeting Nigerians is required to comply with the Rules.

Operators of Digital Asset Offering Platforms (DAOPs) who are the persons responsible for administration of electronic platforms for offering digital assets. In addition to the requirements to put in place rules and procedures that ensure proper functioning of the platform, DAOPs are required to conduct a critical assessment of the Issuer's capacity to deliver the project to be financed, the Issuer's compliance with applicable regulations, confirm the suitability of the senior management team and ensure that potential investors can access white paper containing information on the securities offered on their platforms.

4.1.2. Dealers in Digital Assets

The Rules put in place specific rules intended to achieve consumer protection while ensuring market integrity. Some notable unique protections have been

[42] Securities and Exchange Commission Nigeria, New Rules on Issuance, Offering Platforms and Custody of Digital Assets, 2022.

[43] New Rules on Issuance, Offering Platforms and Custody of Digital Assets, supra n 42, Part A paragraph 2.0.

[44] New Rules on Issuance, Offering Platforms and Custody of Digital Assets, supra n 42, Part D, paragraph 1.1b) .

enshrined within the Rules include a) Moratorium on Issuer Equity Holding by which issuers are required to maintain fifty percent (50%) equity holding post issuance of the digital assets until completion the project being financed by the digital asset offering; and b) restriction on the funds that an issuer can raise through a Digital Asset Offering which is limited to twenty times (20x) the Issuer's shareholder funds.

The Rules demonstrate that there has been a deliberate effort to provide for crypto securities within the existing regulatory frameworks while addressing technology specific risks and putting safeguards that guarantee investor trust/confidence.

The discussion in the foregoing sections shows that the wheel of regulation does not actually have to be reinvented. Regulators simply need to create specific regulation to address crypto-specific risks while succouring the players in the crypto-sphere to find their place within the financial services sector.

Principal Considerations for Development of a Comprehensive Legal and Regulatory Framework for Crypto-Securities in Uganda

In their current form, the applicable Ugandan laws permit unrestricted transfers of public securities between private persons. The question therefore is whether the existing law already accommodates the idea of transfer simply by delivery. In this respect, DLT-securities are akin to the traditional concept of bearer securities.[45] The Companies Act, No. 1 of 2012 envisages a possibility of a company issuing a warrant with respect to fully paid up shares that can be transferred by delivery and would entitle the bearer to payment of the future dividends on the shares included in the warrant.[46] Consider the idea of an electronic bearer security. It bestows the advantages of direct holding of the security by the investor; minimises the risk of loss or theft that was associated with negotiable bearer instruments and enables the investor to transfer their property without the need for intermediation.

The definition of an electronic bearer security need not differ from the accepted characteristics of securities. The Capital Markets Act provides a definition of securities[47] which includes the traditional classes of securities and an all-catching phrase 'any instruments commonly known as securities. This definition gives plenty of liberty to the regulator to extend the law to issuance of any instrument, regardless of form, that can be characterised as a security. Taking the cue from the Kenyan High Court in Wiseman Talents v. Capital Markets Authority-K[48], we can adopt a substance over form approach would easily wrap the new breed of securities within the existing regulatory framework.

Regarding market actors, the approach would be to extend regulation to all actors/participants whose role mimics recognised securities market players. In several countries, policy makers have adopted a technology neutral approach to regulation of the players focussing on the nature of activity.[49] As such, for issuers of DLT- based securities must be required to comply with the existing regulatory framework for securities issuance. Issuers should not be allowed to issue securities without making necessary risk disclosures and giving assurances to potential investors.

[45] Philip Paech (2016), supra n 14. See also Edmund Schuster supra n 9 at p.9.
[46] The Companies Act, No. 1 of 2012, s. 95.
[47] The Capital Markets Act, Cap. 84 2000, s. 1(hh)
[48] Wiseman Talents v. Capital Markets Authority-K (2019) supra n 23
[49] OECD (2021) supra n 26 at p.3

An example can also be drawn from the reasoning of the learned judge in Lipisha Consortium and BitPesa Limited v. Safaricom Limited[50] in reaching the conclusion that the 2nd Petitioner was conducting cross border money remittance business. Although the medium used to receive monetary value was Bitcoin, an unrecognised asset, the activity was still within the statutory definition of money remittance business because monetary value was being received from various countries in the world and converted into local currency.[51] The same ratio decidendi can be seen in the Wiseman Talents[52] decision where the court analyzed the issuer's literature to reach the conclusion that the issuer was in effect offering securities to the public.

Certainly, some challenges will arise regarding regulation of any non-resident players in the eco-system. Upon establishment of the foundational DLT platform, it is inevitable many other eco-system players will emerge including custodians, wallet providers and brokers. Given that the platform would be distributed, there is no limitation on the physical location or jurisdiction of operation. As such regulation must be adapted to regulate those players that are located out of the country but have dealings relating to securities on the local DLT-platform. CMA can draw inspiration from the new Rules issued by the Securities and Exchange Commission of Nigeria to provide guidance on issuance of Digital Assets as Securities.[53] The application of the Rules is extended to '…foreign or non-residential operators that actively target Nigerian investors directly or through their agents, through promotions, publications in Nigeria or direct e-mails to Nigerian addresses'. This would deal with regulatory arbitrage where players make be drawn to set up offshore special purpose vehicles to escape regulatory scrutiny.

In addition, the proposed DLT trading environment will require supporting infrastructure enabling contemporaneous payment and delivery of securities. Fin-tech innovations are characteristically overlapping and mutual reinforcing.[54] Existing innovations can be tailored to provide for contemporaneous payment and delivery of purchased securities on DLT platforms. This would be possible where the platform has a payment option in place allowing for automated payment, (whether using e-money tokens or any other form of e-money), at the time of delivery of the securities. In this respect, there will be need to need to structure the operational environment that is interoperable. The puzzle to be solved would come down to how to integrate the payments system within the DLT platform.

It is not entirely farfetched to explore the idea of creation of tokens that are transferable and accepted on the DLT platform as consideration for securities. The National Payments Systems Act, 2020 allows for issuance of tokens by a Payment Service Providers which are an electronic equivalent of money.[55] Therefore tokens maybe network restricted tokens or e-money tokens that can be accepted even outside of the network.[56] In the case of e-money tokens, money or value is

[50] High Court of Kenya (Constitutional and Human Rights Division) Petition No. 512 of 2015
[51] Lipisha Consortium and BitPesa Limited v. Safaricom Limited (2015) supra n 50
[52] Wiseman Talents v. Capital Markets Authority-K (2019) supra n 23
[53] New Rules on Issuance, Offering Platforms and Custody of Digital Assets, 2022, supra n 42
[54] Dong He et al (2017) supra n 15.
[55] National Payment Systems Regulations, 2021 regulation 3 provides that Payment Services Provider licence can be issued in three categories including payment services including tokens.
[56] OECD (2021), supra n 26 on the need to settle in central bank money (CBDC) or through a tokenised form of central bank currency in order to achieve settlement finality.

purchased from an issuer (bank or other non-bank e-money issuer) and the value is then stored in a digital form on the consumer's personal computer and the notational value can be transferred over the internet.[57]

Free transferability between holders and secondary buyers implies that there should be embedded within the law a mechanism for the protection of buyers of securities from the risk of unauthorised transfers. In the absence of such rules within the legal system, prospective transferees would reduce the price of the securities proportionately to account for the risk of unauthorised transfers. Eva Micheler advances the argument that transfer rules can have an impact on the price which market participants pay for securities: market participants allocate the risk arising out of unauthorised transfers and defective issues between the buyer and the seller.[58] It is therefore important to develop rules that guarantee the indefeasibility of the holder's titles to a reasonable degree.

Regulatory and judicial oversight should also be exercisable over the DLT-based securities trading platform for adjudication of disputes. As a matter of necessity, the design of the DLT based system must provide a route for implementation and/or enforcement of regulatory and judicial decisions. Schuster suggests that an inevitable design choice has to be made when setting up any DLT-based system as a record for public assets: the design must provide room for synchronisation of the records on the DLT-based database with the state of affairs as dictated by the law.[59] This would necessitate a system by which transfers, or other transactions carried out in accordance with the code governing the DLT protocol, but deemed unacceptable by the applicable law, can and reliably will be reversed at the direction of a court.[60] This is a critical area for deliberation because the consequences of illegal transactions subsisting on the distributed ledger is that subsequent buyers would be adversely affected by defects in title of the previous owners.

The proposed solution is therefore to have a third-party prescribing rule for completion of transactions and authorising updates to the ledger.[61] This solution tinkers with the belief that any form of intermediation can be eliminated from financial transactions. Ultimately the integrity of any offering of securities or other investment option to the public depends on the existence of a trusted and credible central authority that will guarantee that the issuer of the tokens is sound and/or the assets backing of the tokens are valuable. As such complete dis-intermediation is not a plausible option but a design can be made that significantly reduce the levels of intermediation and makes transaction execution more efficient.

The existing application of DLT have revealed some deficiencies relating to scalability of the technology. Reports highlight that in their implementation, DLTs prompt further challenges including scalability of the DLT for mainstream use comparable to and exceeding existing non-DLTs performing similar functional

[57]Anita Ramastry, 'Non-bank Issuers of E-Money: Prudential Regulation in Comparative Perspective (2004) in International Monetary Fund, 'Current Development in Monetary and Financial Law', Vol. 4.

[58] Eva Micheler (2010) supra n 25.

[59] Edmund Schuster (2019) supra n 9.

[60] Edmund Schuster (2019) supra n 9.

[61] Edmund Schuster (2019) supra n 9 on the distinction between permissioned and permissionless types of DLT.

tasks.[62] As such in implementation, the Regulator would need to consider subjecting the DLT to stress testing to gauge its ability handle trading volumes.

The discussion on the role of the regulator and the regulatory approach cannot be exhausted in this paper. Even after the innovation has introduced into the market, new risks will be identified in the operational environment. The key focus for the regulator should be to comprehensively provide for known risks and be flexible to address other risks arising in the live environment.

CONCLUSION

We cannot underscore the importance of regulatory support to the innovative process in any sector. In the context of this paper, the anticipated effect of a responsive regulatory environment is that private players will be emboldened to develop legitimate DLT-based asset activities and business models. Equally important is legal certainty: this is as provided by a clear and predictable legal framework, both in the context of public law (that is regulation) and private law (contractual and property law).[63] Drawing from experiences of other jurisdictions, deployment of any form of technology does not necessitate rethinking of the entire regulatory framework. A technology neutral approach could be adopted where the same rules apply to the same types of activities and risks, irrespective of the technological medium through which the product/service or activity is provided[64] A gap analysis would be necessary for purposes of identifying any special rules that should be put in place to manage the risks introduced by the digitalization of aspects of securities transaction.

[62] Leon Perlman (2020) supra n 5.
[63] Dong He et al (2017) supra n 15.
[64] OECD (2021), supra n 26.

LEGAL CONSIDERATIONS OF ADOPTING CENTRAL BANK DIGITAL CURRENCIES IN THE EAST AFRICAN COMMUNITY

Uche Anyamele*

ABSTRACT

In June 2021, the East African Community (EAC), which includes the Democratic Republic of Congo, the United Republic of Tanzania, the Republic of Kenya, Burundi, Rwanda, South Sudan and Uganda, expressed interest in exploring the potential of a Central Bank Digital Currency (CBDC) for their shared payment system. This move was made recognising that a digital, central currency would help deal with members' reluctance to trade in each other's currency. Thus, adopting a CBDC in the EAC could provide an option for EAC members who wish to adopt a single currency in the system by 2024, in line with the bloc's monetary union protocol.

Whilst a CBDC in the EAC could be a game-changer, it is a novel technology requiring a robust legal framework that supports its issuance and can address issues that will arise in the future. The timing of the EAC in considering CBDCs is propitious, given the Community's goal to introduce the single currency by 2024 and the ongoing plans in line with this for the East African Monetary Institute (EAMI), a precursor to the East African Central Bank. A critical question in issuing CBDCs is whether the provisions of the central bank laws directly or indirectly support its issuance. With plans to establish the EAMI, this question need not be asked because the draft law of the EAMI can directly include provisions that support the issuance of digital currency in the EAC.

Considering the above, this paper will consider how the EAC can incorporate provisions that support the issuance of CBDCs in the EAC. The paper will also consider how the CBDC can be designed for the EAC, bearing in mind the legal implications of such designs. The policy goals as well as the attendant risks of issuing CBDCs in the EAC will be examined to determine whether CBDC is suitable for the Community.

* LLM, PhD (Durham). Uche is a legal consultant with varied experience across different jurisdictions. She provides legal advisory and consulting services to different organisations. Her expertise is in international trade (law, policy, finance). Uche researches and writes on the African Continental Free Trade Area (AfCFTA), digital law, including blockchain technology and central bank digital currencies CBDCs.

INTRODUCTION

At least 80% of central banks in the world are considering issuing Central Bank Digital Currencies (CBDC)s.[1] This indicates a real interest and belief in the potential of CBDCs. CBDCs are an opportunity for central banks to align themselves with the digital payments revolution while retaining control over monetary policy.

Recently, East Africa Community (EAC) member states declared their intention to explore the potential of a CBDC for their paid payment system. This decision was primarily motivated by Partner States' reluctance to trade in each other's currency.[2] A CBDC has the potential to deal with this issue given its neutrality and digital nature. Accordingly, adopting a CBDC could provide an option for the EAC Partner States, whose target is to attain a single currency for the region by 2024, in line with the bloc's Monetary Union Protocol.[3]

A common digital currency in the East African Bloc is in line with the aspirations of the Community's objectives stated in Article 5(1), to "develop policies and programmes aimed at widening and deepening co-operation among the Partner States in political, economic, social and cultural fields, research and technology, defence, security and legal and judicial affairs, for their mutual benefit".[4] A CBDC will especially ensure that there is deeper economic and social cooperation in the EAC by providing a safer form of money in an increasingly evolving digital world. The CBDC can also ensure inclusion for vulnerable and unbanked citizens in the EAC as the use of cash gradually declines. There are broader benefits to adopting a CBDC, such as innovation, which could ultimately increase choice, competition, and accessibility to digital payments. A digital currency is also an avenue to reduce the environmental costs of a paper-based monetary system. In adopting a digital currency in the EAC, it will be necessary to ensure that unforeseen and unwelcome consequences are considered, and that proper measures are put in place to address this.

Most concerns with respect to issuing CBDCs revolve around law and regulation. Given this, the paper will primarily examine the legal implications of issuing a CBDC in the EAC. After this introduction, section 2 provides a brief overview to the EAC and CBDC. There is also an outline of the background to the EAC, a brief explanation of the four integration pillars of the EAC and the legal instruments governing the EAC. Section 3 examines the interaction between CBDCs and the regional bloc, including the policy goals, costs, and implications of issuing a CBDC. In this section, I consider the legal implications of different designs and variants of the CBDC and what they mean for the EAC. In section 4, I conclude the paper and provide some recommendations.

[1] PwC, 'Global CBDC Index and Stablecoin Overview 2022:Singapore Highlights' (*PwC Research and Insights*) https://www.pwc.com/sg/en/publications/global-cbdc-index-and-stablecoin-overview-2022.html accessed 19 July 2022.

[2] Allan Odhiambo, 'EAC Explores Potential of Common Digital Cash' The East Africa (Kenya, 2 June 2021) https://www.theeastafrican.co.ke/tea/business/eac-explores-potential-of-common-digital-cash-3422726 accessed 19 July 2022.

[3] Ibid.

[4] See Article 5(1).

1. OVERVIEW OF THE EAC AND CBDCS

Countries wishing to issue CBDCs often, have to justify their motivations. It is therefore necessary to understand the context in which the EAC seeks to issue a CBDC. This context is anchored in the background, nature, and history of the EAC. In the same vein, a brief overview of CBDCs is necessary because as a new and technical concept, it is necessary to ensure that there is a basic understanding of what a digital currency of the central bank means, and how it will operate. In this section, I provide a broad overview of the EAC, what the community is and how it functions. Then I go on to present a broad overview of CBDCs, what it is, its core features and the designs available.

1.1. The EAC

The EAC is a regional intergovernmental organisation with an estimated population of 177 million people.[5] There are seven Partner States, including The Democratic Republic of Congo, the Republics of Burundi, Kenya, Rwanda, South Sudan, Uganda and the United Republic of Tanzania.[6] The Treaty establishing the EAC Community was signed on 30 November 1999,[7] and it entered into force on 7 July 2000 after three Partner States – Kenya, Uganda and Tanzania ratified it. Subsequently, on 18 June 2007, the Republic of Burundi and the Republic of Rwanda acceded to the Treaty. The Republic of South Sudan became a full member on 15 August 2016 whilst the Democratic Republic of Congo acceded to the EAC treaty on 8 April 2022.[8]

The EAC is headquartered in Arusha, Tanzania and its vision is to be a 'prosperous, competitive, secure, stable and politically united East Africa: and provide a platform to widen and deepen Economic, Political, Social and Culture integration in order to improve the quality of life of the people of East Africa through increased competitiveness, value-added production, trade and investments'.[9] Art 5(1) provides the aims and objectives of the EAC which is to widen and deepen cooperation among the Partner States in political, economic and social and cultural fields, research and technology, defence, security and legal and judicial affairs for their mutual benefit. To accomplish this, the EAC established a Customs Union in January 2005 and established a Common Market in July 2010, a Monetary Union in 2012 and ultimately, a Political Federation of the East African States.

[5] East African Community, 'Quick Facts about EAC' (eac.int) < https://www.eac.int/eac-quick-facts > accessed 9 August 2022.
[6] East African Community, 'EAC Partner States' (eac.int) < https://www.eac.int/eac-partner-states > accessed 9 August 2022.
[7] Treaty for the Establishment of the East African Community (the Treaty).
[8] East African Community, 'Overview of EAC' (eac.int) https://www.eac.int/overview-of-eac > accessed 19 July 2022.
[9] Ibid.

1.2. The EAC Integration Pillars

There are four integration pillars on which the EAC seeks to achieve its ambitions.

1.2.1. Customs Union

The Customs Union came into force in 2005 when the Partner States agreed to establish a free trade (or zero duty) imposed on goods and services among themselves, and they have agreed on a common external tariff (CET) to be charged for imports which come from outside the EAC zone when sold to any EAC Partner States.[10] As a result of the Customs Union Protocol, trade has been enhanced in the EAC, making it an attractive place for foreign investment. Some of the key initiatives of the Customs Union include the Single Customs Territory which involves interconnectivity of customs systems to facilitate seamless flow of information between customs stations and a payment system to manage revenue transfer in Partner States. There is also the COMESA-EAC-SADC tripartite that consists of 26 member countries to accelerate economic integration for the Eastern and Southern African Region, the African Growth Opportunity Act (AGOA) the cornerstone of the U.S. economic engagement with Sub-Saharan Africa, EAC-EU Economic Partnership Agreements, and the European Union Everything but Arms.[11]

1.2.2. Common Market

The Common Market, which is the second Regional Integration milestone of the EAC came into force in 2010. To accelerate development, the EAC Partner States adopt a liberal stance towards the four Freedoms of movement for all factors of production. These Freedoms and Rights include Free Movement of Goods, Free Movement of Persons, Free Movement of Labour/Workers, Right of Establishment, Right of Residence, Free Movement of Services, Free Movement of Capital. Underlying the EAC Common Market are operational principles of the Community, namely: Non-discrimination of nationals of other Partner States on grounds of nationality; Equal treatment to nationals of other Partner States; Ensuring transparency in matters concerning the other Partner States and Share information for the smooth implementation of the Protocol.[12]

1.2.3. The Monetary Union

Five East African countries joined forces in 2000 to form a single currency area, the East Africa-Monetary Union (EAMU). These countries, Kenya, Uganda,

[10] World Bank, 'Enhancing Access to Finance for EAC Women Cross-Border Traders' (World Bank Group, July 2021) < https://openknowledge.worldbank.org/handle/10986/36209?locale-attribute=en > accessed 4 August 2022.

[11] East African Community, 'Customs Union' (eac.int) < https://www.eac.int/customs-union > accessed 9 August 2022.

[12] East African Community, 'Common Market' (eac.int) < https://www.eac.int/common-market#:~:text=What%20is%20the%20Common%20Market,fully%2Dfledged%20in%20January%202010> accessed 4 August 2022.

Tanzania, Burundi and Rwanda have been preparing the way for greater economic integration, with plans to have a currency by 2024. The EAMU Protocol was adopted in accordance with the EAC treaty and signed on 30th November 2013. It lays the groundwork for a monetary union within 10 years and allows the EAC Partner States to progressively converge their currencies into a single currency in the Community. To achieve a single currency, the EAC countries must aim to harmonize monetary and fiscal policies; harmonize financial, payment, and settlement systems; harmonize financial accounting and reporting practices; harmonize policies and standards on statistical information and establish an East African Central Bank.[13]

1.2.4. Political Federation

As the fourth step following the pillars above, the Political Federation is the goal of the EAC regional integration and is intended to be a process and not a single event. This pillar seeks common foreign and security policies, good governance, and effective implementation of the other pillars of regional integration. The office of the deputy secretary-general is responsible for the Political Federation was established in 2006. In 2017, the EAC adopted the Political Confederation as a transitional model of the East African Political Federation.[14]

1.3. ORGANS OF THE EAC

There are main Organs of the EAC comprising of the Summit, which is composed of the Heads of State and Government of Partner States. These organs provide strategic direction towards the realisation of the Community's objectives. The Council of Ministers is the central decision-making and governing body of the Community, and the Coordinating Committee is responsible for regional cooperation and coordination of sector-related activities. There is also the Sectoral Committees, responsible for conceptualising programmes and monitoring their implementation, the Secretariat which is the executive organ responsible for initiating and coordinating the harmonisation of policies and strategies relating to the development of the Community; the East African Court of Justice; and the East African Legislative Assembly. In addition, there are several semi-autonomous EAC Institutions which assist in implementing specific areas of the Community's mandate.[15]

In terms of regional strategies and policies, EAC Partner States agreed to coordinate their economic policies with the aim of creating conditions beneficial for developing and achieving the Community's objectives. These objectives are largely to accelerate harmonious and balanced development and sustained expansion of economic activities for their mutual benefit. In the 5th EAC Development Strategy, 2017-2021, the overall goal was to build a firm foundation for transforming the EAC into a stable, competitive lower-middle income region. In achieving this, certain priority areas were delineated including, the development

[13] World Bank 2021 (n 10).
[14] Ibid.
[15] TRALAC, 'EAC Legal Texts and Policy Documents' (*tralac.org)* <https://www.tralac.org/resources/our-resources/4812-eac-legal-texts-and-policy-documents.html> accessed 9 August 2022.

of regional infrastructure.[16] A regional CBDC could fit within this objective because it is an infrastructure that could help increase financial inclusion in Partner States by providing access to finance and financial services to vulnerable citizens and MSMEs. This could ultimately help in improving their living conditions and livelihoods from poor to lower-middle class.

2. CENTRAL BANK DIGITAL CURRENCIES

2.1. What is a CBDC?

There have been attempts to define CBDCs which has resulted in a consensus on key features and some accepted definitions. The Committee on Payment and Market Infrastructure (CPMI) stated that "CBDC is not a well-defined term. It is used to refer to several concepts. However, it is envisioned by most to be a new form of central bank money. That is, a central bank liability, denominated in an existing unit of account, which serve both as a medium of exchange and a store of value."[17] A CBDC can also be defined as a 'digital form of central bank money that is different from balances in traditional reserve or settlement accounts."[18] The International Monetary Fund (IMF) defines CBDCs as "a new form of money, issued digitally by the central bank and intended to serve as legal tender."[19] From these definitions, certain characteristics of CBDCs are evident. CBDC is new, is money, is digital, and emanates from the central bank.

Central banks typically issue two types of money - physical cash and electronic central bank deposits (reserves). There is an infrastructure to support a third, – private money. Whilst cash is widely accessible and peer to peer, central bank deposits are usually electronic and offered to qualifying institutions and private money is usually accessible through electronic commercial bank deposits.[20] CBDCs are therefore a new type of central bank money.

As CBDCs are gaining momentum, some banks agreed to common grounds to govern them, these include: the need for CBDCs to co-exist with cash and other types of money flexibly; the fact that CBDCs should support wider policy objectives; central banks in issuing CBDCs must be mindful of the need not to unintentionally harm monetary and financial stability and in issuing CBDCs there should be a need to promote innovation and efficiency.[21] These are all factors that

[16] EAC, 'EAC development strategy (2016/17 - 2020/21): accelerating a people-centered and market-driven integration' *(Repository.eac.int*, March 2018).
<http://repository.eac.int/handle/11671/1952> accessed 9 August 2022.

[17] Bank for International Settlement (BIS) and Committee on Payments and Market Infrastructures Markets Committee 'Central Bank Digital Currencies' (March 2018)
<https://www.bis.org/cpmi/publ/d174.pdf> accessed 2 August 2022.

[18] Ibid.

[19] Tommaso Mancini-Griffoli and others, 'IMF Staff Note - Casting Light on Central Bank Digital Currency' (2018).
<https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233 > accessed 2 August 2022.

[20] Bank for International Settlement, 'Central Bank Digital Currencies: Foundational Principles and Core Features' (Oct 2020) < https://www.bis.org/publ/othp33.htm> accessed 20 January 2022.

[21] The collaboration between the Bank for International Settlements (BIS) and seven major central banks from around the world - the Bank of Canada, the ECB, the Bank of Japan, Sveriges Riksbank, the Swiss National Bank, the Bank of England, and the Federal Reserve System (Board of Governors) led to the publication of a report on foundational principles and core features of central

must be considered as the EAC prepares to issue CBDCs.

2.2. Prerequisites for Issuing a CBDC

Certain considerations are necessary before a CBDC can be issued. These considerations would be particularly relevant for the EAC as it begins preparations for establishing the monetary institute. Most of the questions which the EAC would have to answer with respect to CBDCs revolve around money and state. Firstly, the EAC would need to establish whether there is a legal basis for issuing a CBDC. Then, it must be ascertained whether specific community laws need to be amended to make provision for issuing CBDCs and whether the central bank or yet-to-be-established Monetary Institute has the authority to issue a digital currency.

Other issues to be examined include how CBDCs would interact with concepts such as Know Your Customer (KYC), data privacy and protection, governance issues and dispute resolution. These issues related to the EAC are addressed in the paper.

3. THE EAC AND CBDCS

There are many considerations in issuing a CBDC in EAC. Consequently, it is necessary to understand the policy goals for issuing a CBDC in the regional bloc, the attendant risks of issuing a CBDC, the design implications of different CBDCs and its suitability to the policy goals of the EAC. In the same vein, it is necessary to consider the legal basis and authority for issuing the CBDC in the EAC whilst examining how the CBDC will work with other concepts.

3.1. Policy Goals of the EAC in Issuing CBDCs?

3.1.1. Overcoming reluctance of trading in Partner States' currency by trading with a neutral currency

A primary reason why the EAC is considering issuing CBDCs is that they would eliminate the need for the Partner States to trade in each other's currency. The EAC plans to have a single currency by 2024. Five East African countries joined forces in 2000 to form a single currency area, the East Africa-Monetary Union (EAMU). These countries, Kenya, Uganda, Tanzania, Burundi, and Rwanda have been preparing for greater economic integration. The EAMU Protocol was adopted in accordance with the EAC treaty and signed on 30th November 2013. The Protocol lays the groundwork for a monetary union within ten years and allows the EAC Partner States to progressively converge their currencies into a single currency in the Community.[22]

There are benefits and costs to the use of common currency. A monetary union

bank digital currencies, European Central Bank, 'ESCB Legal Conference 2020' (Frankfurt am Main, Germany, 11 September – 2 November 2020) https://www.ecb.europa.eu/pub/pdf/other/ecb.escblegalconferenceproceedings2020~4c11842967.en.pdf> accessed 2 August 2022.

[22] East African Community, 'Monetary Union' (*eac.int*) https://www.eac.int/monetary-union#:~:text=The%20EAMU%20Protocol%20was%20adopted,single%20currency%20in%20the%20Community > accessed 2 August 2022.

is useful because it could help with the elimination of transaction costs of exchanging currencies and removing the exchange rate volatility. The main cost of monetary union is the inability of monetary authorities of the individual countries to use country-specific monetary policies and the exchange rate as an instrument of macroeconomic adjustment in response to shocks.[23]

The EAC launched the East African Payment System (EAPS) in May 2014. Since then, it has been plagued by members' reluctance to trade in each other's currency, leaving Kenya to control over 98 per cent of the transactions through the system. As of 2019, Kenya dominated transactions in the EAPS.[24] The agreement to make all regional currencies tradable was signed in 2014 by the EAC member states because they aimed to promote intra-regional trade and prepare for a monetary union by 2024. Even though EAC central banks have opened reciprocal accounts with each other, member countries are still reluctant to pay and receive payments in regional currencies.[25] In this regard, because CBDCs use electronic records or digital tokens to represent a fiat currency of a region, they are neutral and independent of any member state's currency. Furthermore, since digital currency will be centralised, issued, and regulated by the monetary institute of the EAC, it would remove any preference for any member state's currency.

3.1.2. Reducing and eliminating operational and financial inefficiencies

Most central banks issue a CBDC because of the possibility of making payments more efficient. In particular, central banks of emerging market economies ranked payments safety and domestic payments efficiency as the first motivating factor for issuing either a wholesale or retail CBDC.[26] CBDCs can make payment systems seamless by reducing transaction costs and increasing the speed of transactions. This would be directly beneficial for cross-border payments because their remittances would be improved. Cross-border payments are often costly and time-consuming because there are several intermediaries. The time lag in such transactions exposes counterparties to credit and settlement risks. Moreover, multiple friction points exist in cross-border transactions such as 'fragmented and truncated data formats, complex processing of compliance checks, limited operating hours and legacy technology platforms.[27] Having a CBDC system that is interlinked with other systems could deal with this issue. Additionally, of the problems with the EAPS is that its functionality is reduced because there is no

[23] 'The East African Monetary Union: Ready or Not?', UN. ECA Intergovernmental Committee of Experts (ICE) Meeting (21st: 2017, Nov. 07-09: Moroni, Comoros) (United Nations Economic Commission for Africa Subregional Office East Africa (SRO-EA) 2022) <https://repository.uneca.org/handle/10855/24078> accessed 8 September 2022.

[24] James Anyanzwa, 'EAC to upgrade underperforming e-payment system' (*The East African Kenya*, 3 August 2019) https://www.theeastafrican.co.ke/tea/business/eac-to-upgrade-underperforming-e-payment-system-1424186 accessed 4 August 2022.

[25] Ibid.

[26] World Bank, 'Central Bank Digital Currency: A Payments Perspective' (*World Bank*, 2021 Washington, DC. World Bank) <https://openknowledge.worldbank.org/handle/10986/36765> accessed 9 August 2022

[27] Shehnaz Ahmed, 'Will CBDCs help ease cross-border payments' (*The Economic Times India*, 20 September 2021) https://m.economictimes.com/markets/cryptocurrency/will-cbdcs-help-ease-cross-border-payments/amp_articleshow/86361778.cms accessed 9 August 2022.

automated mechanism to confirm that messages sent by the local commercial banks have been received and settled in the respective central banks. This ultimately results in delays in receiving feedback on the settlement of transactions from the regional counterparts.[28] CBDCs can help in that they are instantaneous, fast, and automated. This can help improve the functionality aspects of transactions.

3.1.3. Addressing financial inclusion

CBDCs are also a way to ensure financial inclusion for the unbanked and underbanked. This will ensure they have access to a broad range of financial services.[29] In a survey conducted by the Bank for International Settlements (BIS) amongst banks from developed and emerging economies regarding their motivation for issuing CBDCs, financial inclusion emerged as the main factor for CBDC development.[30] Currently over 1.7 billion adults worldwide are excluded from the formal financial system. In Africa, more people are excluded from financial services because of income disparity. CBDC can enhance financial inclusion by providing a means of entry to the digital economy because it gives a payment option that can be used anywhere by anyone. Issuing CBDCs can also help promote financial innovations by providing innovative investments and financing tools and schemes deriving from open banking and open finance. CBDCs can also support e-Government initiatives since their issuance facilitates digital transformation in all economic fields including the public sector.

3.1.4. Enhancing payments system

The present EAC payment system is plagued by difficulties in funding arrangements of the regional currencies from regional commercial banks.[31] 'The original funding model where participants sourced for funding of other EAC currencies from the market has become expensive due to unavailability of Partner States currencies in the local market'.[32] Using CBDCs can be less expensive because there would be a central digital currency which eliminates the need for availability of the Partner States' currencies in the local market.

3.1.5. Digitalising the EAC economy

As the world becomes more digital, it is imperative for countries and trade blocs to become digitalised. Economies world over are increasingly becoming interested in converting traditional financial securities and other physical assets into digital

[28] Odhiambo (n 2).
[29] Sarah Allen and Others, 'Design Choices for Central Bank Digital Currency: Policy And Technical Considerations' (2020) Global Economy & Development Working Paper 140 <https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf > accessed 4 August 2022.
[30] Codruta Boar and Others,' Impending Arrival – A Aequel to the Survey on Central Bank Digital Currency' (2020) BIS Papers No 107 <https://www.bis.org/publ/bppdf/bispap107.pdf > accessed 2 August 2022.
[31] Anyanzwa (n 24).
[32] Odhiambo (n 2).

assets that can be bought, sold, and exchanged, using newer models of trading infrastructure based on blockchain technology. Issuing a CBDC is one way to encourage the digitalisation of the EAC economy. CBDCs can therefore encourage the development of innovative solutions for the EAC trade industries. With a CBDC, gaps in the digital payment solution and functionalities of the EAC could be resolved. CBDCs can also provide a digital variant of central money for use as a settlement asset and mitigate primary risk by 'allowing delivery-versus-payment and payment-versus-delivery functionality for digitalised financial assets'.[33] Depending on the design of the CBDC - for instance a retail CBDC - it would be available to the public and would also support the digitalisation of the financial sector and the broader economy of the region. Payment service providers and banks would enjoy reduced costs since their business process would be more efficient and supportive of new business models. Where a CBDC is adopted in the EAC, it must be flexible enough to allow it to evolve and keep up to date with the evolving technology landscape so that it can be current enough to address the needs of the EAC market. Any CBDC must be usable, convenient, fast, cost-efficient, and programmable. It is therefore recommended that such CBDC must be interoperable with private payment solutions and available through front-end solutions throughout the EAC region.

3.1.6. Ensuring continued access to central bank money in the face of declining cash usage

Technology is spurring rapid changes in the monetary and payment systems globally, and e-commerce is rapidly growing. As a result, currency is undergoing a transformation in significant ways. The COVID-19 pandemic also increased the need for digitalisation of payments and contactless payments systems in developed and developing economies.[34] A decline in cash usage suggests an increasing dependence on private forms of money and private payment solutions. Where cash is in decline, there is the danger that households and businesses will no longer have access to risk-free central bank money because cash infrastructure will no longer be sustainable thus, resulting in problems with providing adequate cash services. Central banks consider it important to provide public access to money.

That the public has access to central bank money is vital in order to develop confidence in the currency.[35] Issuing a CBDC which is like a digital banknote could help fulfil this obligation of the central bank to provide public access to money in the EAC. A digital banknote in the EAC would be an additional form of public money and means of payment. The characteristics of cash are such that its physical nature, privacy, autonomy, and independence from technical infrastructure make it attractive.[36] Such benefits cannot be fully matched by a digital note.

[33] World Bank (n 2021).

[34] Katherine Foster and Others, 'Digital Currencies and CBDC Impacts on Least Developed Countries (LDCs)' (2021) The Dialogue on Global Digital Finance Governance Paper Series <https://www.undp.org/sites/g/files/zskgke326/files/2021-06/UNDP-UNCDF-TP-1-2-Digital-Currencies-and-CBDC-Impacts-on-Least-Developed-Countries-LDCs-EN.pd > accessed 4 August 2022.

[35] BIS Foundational Principles (n 20).

[36] European Central Bank, 'Report on a Digital euro' (October 2020) <https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf > accessed 4 August 2022. 9-14.

However, when designed bearing this in mind, it is possible that a CBDC can, to a large extent, replicate many such qualities of cash. Thus, allowing citizens of the Community to be able to continue to make their payments as they do with cash.

3.1.7. Ensuring resilience of payments

One of the benefits of CBDCs is that they can help with paying and extending transfers to individuals under severe circumstances in disaster-prone areas. Countries like the Bahamas and the Eastern Caribbean Currency Union (ECCU) have this as their policy goals in adopting CBDCs because natural disasters are frequent in that region.[37] Based on this advantage, the EAC may be motivated to adopt a CBDC because it could act as an additional payment method that would improve operational resilience where access to cash is marginalised. Normally, cash could be a backup payment method to electronic systems where networks are no longer able to function. However, cash could also be marginalised. In fact, when compared to cash, a CBDC could be a better system to distribute and use funds in geographically remote areas or when there are natural disasters.[38]

However, to fully utilise the CBDCs in this manner, the EAC must ensure that the CBDC has full offline capacities. National payment systems would be safer and more resilient because of CBDCs since it has the potential for faster settlement, greater interoperability, and enhanced money velocity.[39] Furthermore, as the digitalisation of payments grows, there could be concentration risks where there are a few large operators. AliPay and TenPay/WeChat Pay are the largest operators in China, and as noted by the People's Bank of China (PBOC) where such firms fail, it could have serious consequences for the Chinese payment system.[40] There is also a possibility of disruption to digital services. CBDCs can help to deal with this by playing a role as an additional backup especially given the falling cash usage.

3.1.8. Providing a credible alternative as a medium of exchange and potentially a store of value in the Community

Given the growth of the AfCFTA and the fact that other African countries are researching and issuing their CBDCs including China, these currencies could be made available to citizens of the EAC, resulting in currency substitution as well as an increase in foreign exchange risk in the region. With private money payments like stablecoins being developed, there is a likelihood that they would achieve global footprints and become widely used for retail payments.[41] Whilst these payments foster innovation, they could pose a threat to the EAC's financial, economic and political sovereignty.[42] Where the EAC accepts a means of payment

[37] BIS, Innovation Hub Other, 'Central Bank Digital Currencies: Foundational Principles and Core Features' (Oct 2020) <https://www.bis.org/publ/othp33.htm> accessed 20 January 2022.
[38] BIS Foundational Principles (n 20) at 5.
[39] Allen (n 29) at 16.
[40] Gabriel Soderberg and Others, 'Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons' (February 2022) <https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174> accessed 5 August 2022.
[41] Report on the Digital Euro (n 36) 9-16.
[42] G7 Working Group on Stablecoins 'Investigating the Impact of Global Stablecoins' (*Bis.org*, 2022) <https://www.bis.org/cpmi/publ/d187.htm > accessed 5 August 2022.

or store of value that is not denominated in their regional currency of choice it would not only weaken and impair the monetary policy but may have effects on financial intermediation and cross-border capital mobility which could affect financial stability. A regional CBDC could be issued to avoid this.

3.1.9. Reducing illicit use of money and corruption

CBDCs can help reduce illicit financial transactions like money laundering and terrorism and reduce tax evasion because of its traceability. Illicit Financial Flows in Africa and corruption are closely interrelated. Thus, corruption is a source of proceeds, often in the form of bribes.[43] The distinctive features of cash, including its anonymity and lack of an audit trail, make it attractive for illicit transactions such as tax evasion, money laundering and terrorist financing. CBDCs can mitigate this problem because as a legal tender, it is traceable. In terms of the level of secrecy of jurisdictions and their roles in enabling money-laundering, tax evasion and the concentration of untaxed wealth, Kenya, a vital member of the EAC, was ranked 24th of 112 jurisdictions in the Financial Secrecy Index of the Tax Justice Network.[44] CBDCs can enable more transparent transactions in Kenya.

3.2. Risks of Issuing CBDCs in the EAC

3.2.1. Economic risks

The economic risks of issuing CBDCs include inflation and low adoption by consumers and businesses. Inflation occurs when there is a price increase in goods and services which over time reduces the value of the currency. It is caused by a growth in money supply, exceeding the growth in production. CBDCs can cause inflation because it can be created with a press of button and distributed immediately without any reference to a corresponding increase in production.[45] To reduce this risk CBDCs can be issued to individuals and businesses only in return for bank deposits or collateral paid for with bank deposits. In the case of government, it should be issued with respect to bonds that have a significant chance of being repaid through taxes.[46] There could also be large-scale misallocation of capital and effort to implement the CBDC. As part of its considerations for issuing CBDCs, the EAC must bear in mind that consumers may not accept it. The attendant risk that low adoption pose is that significant expenses may have been spent on infrastructure to develop the CBDC and yet the level of adoption will not justify the expense. Where the public is responsible for designing, building and issuing the CBDC, there is a high risk of low adoption due to poor utility, poor execution and poor user experiences. To deal with this, there have been suggestions that the private sector is best positioned to provide the

[43] Melvin D Ayogu and Folarin Gbadebo-Smith, 'Governance and Illicit Financial Flows' in *Capital Flight from Africa: Causes, Effects, And Policy Issues* (S Ibi Ajayi and Leonce Ndikumana (eds), Oxford University Press, 2014) at 11.

[45] Jeremy Light, 'The Risks to Society of Central Bank Digital Currencies' (*Finextra*, 17 January 2022) <https://www.finextra.com/blogposting/21584/the-risks-to-society-of-central-bank-digital-currencies> accessed 8 August 2022.

[46] Ibid.

infrastructure, yet they will need incentives to design CBDCs for public use.

3.2.2. Financial risks (exchange rate risks, higher lending costs and operational risks)

The financial risks associated with CBDCs include exchange rate risks, higher lending costs and operational risks.[47] CBDCs can intensify currency competition and increase the risk of substitution because it will expand the range and supply of attractive and accessible currencies from which people can choose.[48] The unique designs of CBDCs such as interoperability with other financial services and compatibility with smart contracts, as well its network externalities including integration with and across vast online platforms could make it more attractive than traditional sovereign money, to consumers in the regional bloc. The implication for a country would be the widening of the performance gap between a given domestic currency, including a relatively stable one and some new foreign private or digital currency.

Issuing the CBDC in the EAC could result in higher lending costs which could be a consequence of a decrease in banks with CBDC and an increase in more expensive market-based financing and lending costs.

3.2.3. Financial Stability and Financial Inclusion Risk

If the EAC opts for retail direct CBDCs, there would be a declining reliance on banks and payment service providers, which could inhibit the role of banks within the financial system, thus, disrupting the existing financial disintermediation structure. Where this happens, it could result in financial stability and monetary policy risk where there are no measures to address such risks.[49] Currently, in protecting money and providing oversight, the central bank of states do not act as retail banks or technology and service providers. However, a retail direct CBDC would allow central banks and governments operating cash transfers to directly provide to the public.

Additionally, whereas currently, central banks act as lenders of last resort, responsible for bailing out banks and large corporations, with the introduction of retail CBDCs the nature of the relationship between central banks and individuals would change. To deal with this, it is necessary that the EAC considers issuing hybrid CBDCs, where these risks can be avoided by central banks involving commercial banks in the distribution of the CBDC and dealing directly with the customers. CBDCs would bring about increased financial innovation with novel

[47] Ibid.

[48] Markus K Brunnermeier and others, 'The Digitalization Of Money' (2019) NBER Working Paper Series 26300 < https://www.nber.org/system/files/working_papers/w26300/w26300.pdf > accessed 3 August 2022 and Markus Brunnermeier and others, 'Digital currency areas' (cepr.org, 3 July 2019) <https://cepr.org/voxeu/columns/digital-currency-areas> accessed 6 August 2022.

[49] Council of Arab Central Banks and Monetary Authorities Governors, 'Central Bank Digital Currencies: A Practical Guide for Arab Central Banks' (2022) Arab Regional Fintech Working Group <https://www.amf.org.ae/sites/default/files/publications/2022-02/CBDCsA%20Practical%20Guide%20for%20Arab%20Central%20Banks-Feb-2022%20%287%29.pdf> accessed 2 August 2022 at 19.

risks. This may affect employees of central banks who are unlikely to have the capacity to deal with this and inhibit regulators in developing tools and expertise to address such risks.[50]

3.2.4. Security risks: data protection and privacy; theft and cyber attacks

Like any digital payment system, the CBDC is vulnerable to cyber security attack, account and data breaches and theft, as well as counterfeiting. With all of this, the EAC must ensure that citizens are comfortable adopting CBDC by assuring citizens of the level of security. Whilst accessing and transferring funds through the CBDC, there could be a real threat of credential theft and loss, which could compromise accounts, funds and data. This is likely to happen because user credentials could be given in the form of passphrase which can easily be communicated on paper or a hardware that stores the private key.[51] Such theft can be virtual or physical, with perpetrators using high-level resources to extract information from a user's device. Hackers can also attack a central bank's digital verification services centre or third-party terminals maintained by commercial banks.[52] Given this, the EAC should design their CBDC as one that allows recovery of passphrases or hardware tokens if they are lost or damaged in natural disaster.[53]

Blockchain based CBDCs which are would likely have a multi-signature wallet, which allows at least two trusted parties to hold credentials to the same wallet. These wallets are not user friendly since any transfer needs to be coordinated with at least one of the other parties.[54] A CBDC that is user-friendly should be a priority for any African country or region because of infrastructural challenges and digital literacy levels. Additionally, where blockchain technology is used for the CBDC, it is possible that nodes can include central bank entities that have the power to invalidate transactions. Malicious nodes of this level can result in security threats which can undermine monetary authority and independence because they can accept or reject transactions that are contrary to the central bank's intention.[55]

The EAC also needs to design a system that ensures there is a balance between anonymity and the registration of users using their real names because a purely anonymous CBDC could be risky and encourage cyber hackers, money laundering and illicit acts. These sorts of threats can make cash seem preferable since cash does not contain information about the previous owner whereas, digital currencies are determined by the owner's identification code and private key.[56] To mitigate this risk, the EAMI in drafting CBDC regulation, could criminalise unauthorised retrieval of personal information of CBDC account owners making such information confidential.[57] A further concern about CBDC is that certain users like central bank or government insiders, law enforcement and other agents may be able

50 Council of Arab (n 49) at 19.

51 World Economic Forum, '4 Key Cybersecurity Threats to New Central Bank Digital Currencies' (*weforum.org*, 20 November 2021) <https://www.weforum.org/agenda/2021/11/4-key-threats-central-bank-digital-currencies/> accessed 3 August 2022.

52 Council of Arab (n 49) at 19.

53 WEF, 2021 (n 51).

54 Ibid.

55 WEF, 2021 (n 51).

56 Council of Arab Central Banks (n 49) at 19.

57 Ibid.

to take privileged actions as a result of their positions. For instance, they could freeze or withdrawal funds from CBDC accounts without the user's consent.[58] Whilst this sort of privilege is necessary to ensure compliance and for regulatory purposes, it could also be an avenue for insiders to use the information for malicious purposes. The EAMI should ensure that there is protection against this by using methods such as multi-party mechanisms which would make it more difficult to be use for malicious purposes.[59]

3.2.5. Vendor Risk

The EAC in issuing its CBDC is likely to select a technology vendor to provide the technology housing the digital currency. Where the central bank is not involved with the technology there could be systematic risks and incompatibilities. There would be overlooked supply chain operational vulnerabilities and supplier risks.[60]

3.3. Legal Basis for Issuing CBDC in EAC

For the EAC to issue a CBDC, there must be a legal framework stating that the central bank of the EAC has the mandate to issue the CBDC. There should also be a provision on the legal status of the CBDC. Since a CBDC is digital money, issued by the central bank, the critical question becomes whether the central bank of the region has the authority to issue the CBDC because not all central banks have the authority to issue CBDCs. In these early stages of the EAMI, there is an opportunity to include clear provisions in the draft laws allocating the central bank authority to issue CBDCs. The currency issuance function could be broadly worded, and the definition of currency could explicitly include not just banknotes and coins, but electronic money issued by the central bank. Such law should describe the legal nature of the CBDC as well as the roles and responsibilities of the central banks, the relevant competent government entities and the private sector in the design, issuance, distribution, access and continuous support of CBDC.'[61] An example of this is in the revision of the People's Bank of China Law (draft) which suggests that Chinese currency include both digital and physical forms. In the law, it is suggested that the central bank should also have broad powers to plan, organise and supervise the payment system and financial infrastructure. The production, sale and circulation of illegal CBDCs are prohibited and attract a fine.[62]

The IMF identifies two ways that countries can derive powers to issue a CBDC:

- There can be a provision allocating the EAMI functions, tasks, or duties to achieve its objectives.
- Alternatively, there can be a provision that allocates the central bank powers. Such a provision will state how the central bank can act to

[58] WEF, 2021 (n 55).
[59] Ibid.
[60] Ibid.
[61] Xenia Kalogirou, 'Authorities Explore How to Design Central Bank Digital Currencies' (*iflr.com*, 21 January 2022) < https://www.iflr.com/article/2a647e1ubbp4genwpw2yo/authorities-explore-how-to-design-central-bank-digital-currencies> accessed 3 August 2022.
[62] PBOC (2020) Articles 18 and 19; See also Soderberg (n 40) at 18.

implement its functions. [63]

With respect to functions, there are two typical central bank functions pertinent to issuing CBDCs – the currency issuance functions and the payment system function. The currency function allows the central bank to issue money to the national economy. This means that any currency issuance function to be drafted for the EAMI should either permit it to issue all types of currency for the regional bloc, or limit issuance to banknotes and coins. This function would only be relevant for token-based CBDCs since account-based CBDCs are merely balances in cash current accounts which are digitalised in the books of central banks.

On the other hand, there is the payment system function which has to do with the central bank's function to operate and oversee payments systems. The EAMI should have laws drafted in such a way that they are legally authorised to establish a payment system that is open to the public. This is useful for retail, token based CBDCs. For account-based CBDCs, banks are usually only able to open and hold cash current accounts for specific purposes like when acting as bank and banker, for states and operating payment systems.[64] This means that if the EAMI were to issue account-based CBDCs they must consider whether the governing law would provide authorisation for entities outside those authorised by the central banks. Apart from these issues, the EAMI needs to consider whether the CBDC would be accorded a legal tender status. If this is the case, the legal conception of legal tender status should be loose, leaving room for contractual derogations. However, it should be noted that if the CBDC is not widely accepted by the Community it could result in reputational risk for the issuing central bank.[65]

3.4. CBDC Operating Model, Design Features and the EAC

A vital aspect for the EAC to consider is operating model of the CBDC- that is- how to issue and circulate the CBDC, as well as what role the central bank and the private sector will play in issuing the money. consideration should also be Yet, there are also questions of whether the CBDC would be directly available to households or simply accessible to central bank counterparts. Whether the infrastructure would be centralised or decentralised and whether it would be token-based, or account-based. These have to do with the design features of the CBDC. In considering these, it is necessary to evaluate the legal implications of such designs on the EAC. Currently, the Community is still in the phase of establishing a monetary institute, as they converge towards a single currency. This Institute will later serve as the central bank for the region. The establishment of the East African Monetary Institute (EAMI) – the equivalent of a central bank is a welcome idea by Partner States although it is yet to be decided where to host the bank.[66]

---

[63] Wouter Bossu and Others, 'Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations' (2020) IMF Working Paper <https://www.imf.org/-/media/Files/Publications/WP/2020/English/wpiea2020254-print-pdf.ashx> accessed 3 August 2022 at 16.

[64] Ibid.

[65] Soderberg (n 40) at 19.

[66] The Citizen, 'Tanzania intent on Hosting EAC Central Bank amid Objections' (*The Citizen*, 31 July 2022) <https://www.thecitizen.co.tz/tanzania/news/national/tanzania-intent-on-hosting-eac-central-bank-amid-objections-3898104> accessed 5th August 2022 Tanzania's intention on hosting the bloc's monetary institute after winning the verification exercise has been met by objections from

3.4.1. Operating model of a CBDC

The issuance and circulation of CBDC as well as the designated roles of the central bank and private sector constitute its operating model. There are various classifications for the operating model of the CBDC, including direct/one-tier and indirect/two-tier, or unilateral CBDC and intermediated CBDC. [67] The direct/1 tier CBDCs allow the central bank to issue and administer the CBDC themselves. Here, the central bank operates a retail ledger and is involved in all the payments, from issuing the CBDC to distributing it and interacting with end users. Hence, the central bank bears the operational tasks and costs normally associated with user-facing activities which would normally be borne by the private sector.[68] In such a role, the central bank becomes more involved in economic policy like opening bank accounts, account maintenance and enforcement of AML/CFT rules.[69]

The EAC in issuing the CBDC has to consider whether EAMI would be able to perform this function. As the EAMI is still in the early stages, this is a good time to assess and designate its function, bearing in mind certain consequences of the 1 tier infrastructure - including possibilities of stifling innovation and the EAMI assuming a financial intermediation function, which, the private sector is normally better suited to perform. This could result in their assuming a large share of bank liabilities and the possibility of their taking over bank assets too.[70]

Indirect/two-tier systems are structures issued by commercial banks but fully backed by central bank liabilities. Here the central bank and the private sector each play their respective roles, but with the operational tasks on the commercial banks. Thus, the private sector firms including Partner State-owned intermediaries may also be involved and will interact with the end-users.[71] In this model, although intermediaries perform most functions, the central bank still must monitor and regulate the private sector. In terms of *issuing* within this model, the liability of the CBDC can be that of the EAMI, but a private company can own the technical system.[72] For validation of transactions either in the Distributed Ledger Technology (DLT) system or more traditional ones like checking of identity, the authenticity of money and availability of funds, the function can be split between the EAMI and private sector.[73] This model however can be challenging because if the intermediary is in financial problems, it can be a long and lengthy process, with uncertain outcomes to determine the legitimate owner.[74]

A hybrid form of CBDC, which is incorporated in the e-Naira in Nigeria is the one which combines the direct claims on the central bank, but the intermediaries handle payment. This model is convenient because it embodies the convenience of the private sector payment and the authority of the direct claim on the central

Kenya and Uganda.

[67] BIS Annual Economic Report, 'CBDCs: an opportunity for the monetary system' (23 June 2021). < https://www.bis.org/publ/arpdf/ar2021e3.htm> accessed 5 August 2022.

[68] Ibid.

[69] Ibid.

[70] Ibid.

[71] Soderberg (n 40) at 8.

[72] Ibid at 10.

[73] Ibid. See for instance the e-krona proof of concept where central bank performs the function of checking that the money has not been spent before and the private sector does the remaining checks.

[74] It must be said however that such episodes of bankruptcy by intermediaries can be infrequent.

bank.[75]

Two legal issues arise in this scenario – it is necessary that a 'real' CBDC must be a direct liability of the central bank.[76] Thus, any liability of a commercial bank, even if backed by 100% cash deposit in the books cannot be considered a liability of the central bank. CBDCs which take this form are considered synthetic.[77] A synthetic CBDC is another existing but distant option. It is a special type of e-money or stablecoin which is not issued by the central bank but backed by central bank-issued assets.[78] Within this distinction, the question that arises with respect to token-based CBDCs is whether and under what conditions a legal framework will allow deposits of such token-based CBDCs in the books of commercial banks.[79] It is noteworthy that most central banks that have issued CBDCs converge around the indirect/2 tier CBDCs.

3.4.2. Design features for the EAC

3.4.2.1. Retail and wholesale CBDCs

Retail CBDCs are electronic central bank money that like cash is directly available to consumers, households, private entities, and non-financial corporations.[80] Retail CBDCs have the primary purpose of serving as settlement media for retail payment transactions. They modify the conventional two-tier monetary system because through them central bank digital money is made available to the public.[81] Wholesale CBDCs, akin to central bank reserves, are only for use by regulated financial institutions. Wholesale CBDCs build on the two-tier structure where the central bank is at the foundation of the payment, and customer-facing activities are assigned to PSPs. The central bank grants accounts to commercial banks, and domestic payments are settled on the central bank's balance sheet.[82] Wholesale CBDCs are intended for the settlement of interbank transfers and related wholesale transactions. By the fact that they are offered to the public are far-reaching.

It is important to distinguish retail and wholesale CBDCs because legally if a

[75] Raphael Auer and Rainer Boehme, 'The Technology of Retail Central Bank Digital Currency' (BIS Quarterly Review, 1 March 2020).

[76] A synthetic CBDC is where private organisations issue and manage the CBDC however, the central bank backs up the liability. Essentially most of the tasks involved in the CBDC are outsourced to a private company. There would be a public-private partnership between the central bank and private institutions in issuing the CBDC. With respect to a real CBDC, central banks are the operators of the CBDC system and — in the case of an account-based CBDC — offer accounts to the public. For a very simple explanation of this distinction in the context of the Euro area.

[77] BIS CBDC Foundational Principles (n 20).

[78] Soderberg (n 40) at 8.

[79] The legal framework on which claims are anchored and which helps to keep them segregated from the balance sheet of the payment service providers (PSPs) are critical. As a result of such separation where the PSP's go insolvent, consumers CBDC's held in account would not be exposed to claims by creditors of the PSPs. This segregation is what provides credibility to the system. Bossu (n 63).

[80] Raphael Auer and Rainer Böhme, 'CBDC Architectures, the Financial System, and The Central Bank Of The Future' (*CEPR.org,* 29 October 2020) < https://cepr.org/oxeu/columns/cbdc-architectures-financial-system-and-central-bank-future > accessed 5 August 2022.

[81] BIS Annual Economic Report, 'CBDCs: An Opportunity for the Monetary System' (23 June 2021) <https://www.bis.org/publ/arpdf/ar2021e3.htm > accessed 5 August 2022.

[82] Ibid.

CBDC is designed as an account balance in the current account, central banks will normally restrict access to such accounts.[83] One main reason for issuing CBDCs in Africa is financial inclusion. Therefore, for the EAC, a retail CBDC may eb preferred it would allow more public participation. The key consideration for issuing a retail CBDC is that current electronic retail money represents a claim on an intermediary, rather than functioning as the digital equivalent of cash This raises several issues, as the intermediary might run into insolvency, be fraudulent, or suffer technical outages.

3.4.2.2. Account-based or token-based CBDCs

Retail CBDCs can either be token-based or account-based. Generally, money is based on two basic technologies, tokens of stored values or accounts.[84] The distinction between the two is that whilst account-based CBDCs require verifying the identity of the payer, a token-based system requires verifying the validity of the object used to pay.[85] Account-based CBDCs require structuring the CBDC in a way that balances in cash current accounts are digitalised in the books of central banks. An example with respect to a token-based system (which bis also an example of a store of value) is what happens with cash. To verify the validity of the object used in a cash transaction, one would have to worry about whether it is counterfeit.[86]

If it is electronic money, there would be need to check whether all the money is genuine or whether it has already been spent. An example with the account-based system is the Fedwire Funds Service where a participant issues an instruction to transfer money to another participant. Such transfer must be done in accordance with the instructions of the Reserve Bank's security procedure to verify that the instruction is authorised.[87] These procedures limit the chance that the Reserve Bank will act on unauthorised instruction and the likelihood of fraud through the service.[88] The second approach can be helpful in monitoring illicit activity in payments systems. This is particularly useful because of the levels of corruption in African countries. Still, account-based CBDCs do not remove the need to preserve privacy and shield personal transaction data from commercial parties and public authorities where the payment authentication process is well designed.[89] The problem with digital tokens is that there is still uncertainty regarding their legal status under public and private law, whereas the legal status of balances in current accounts is established.[90] A key issue which the EAC must therefore clarify is how to deal with the uncertainty that could arise with issuing token-based CBDCs.

[83] Bossu (n 63).
[84] Edward Green, 'Some Challenges for Research in Payment Systems' in A Haldane, S Millards and V Saporta, Milton Park (eds) *The Future of Payment Systems* (1st edition 2007 Routledge).
[85] Rod Garratt and Others, 'Token- or Account-Based? A Digital Currency Can Be Both' (*Liberty Street Economics New York*, August 12, 2020) https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/> accessed 5 August 2022.
[86] BIS & CPMI 2018 (n 17).
[87] Garratt (n 85).
[88] Ibid.
[89] BIS Annual Economic Report 2021 (n 81).
[90] IMF Staff Note (n 19) at 16.

(a) Legal issues of token-based CBDCs

Although many central banks are authorised to produce, circulate, and withdraw banknotes and coins, it is not all central banks that can issue a CBDC because of its digital nature. The question of authorisation to produce or circulate is primarily related to the token-based variant of CBDCs. In drafting its laws, the EAMI must ensure that such drafting allows for the issuance of token-based currency either through the central bank's function or power. The provision on currency issuance should be worded broadly so as not to limit the central bank's power to banknotes and coins. The currency issuance function should be equally open, or the law can refer to other means of payment other than banknotes and coins.[91]

The EAMI could also opt to draft its law to explicitly authorise the issuance of a CBDC. Such drafting would happen where there is no currency issuance power but a general function to issue currency, without this being limited to banknotes and coins. Such law should not have indirect provisions or specific ancillary powers that will restrict issuance to banknotes.[92]

(b) Legal issues around account based CBDCs

One of the main powers of central banks is the power to open and hold cash current accounts. In this sense, central banks act for specific purposes such as for bank and banker for states and to operate payment systems. An important issue for the EAMI with regard to account based CBDCs is whether the central bank law should be drafted to authorise entities outside those whom the central bank would normally be authorised to open account for? The concern for central banks is that there is usually insufficient legal basis to issue account based CBDCs to the public. At this early stage where the EAMI is coming into force, this issue can be resolved by drafting an explicit provision allowing the issuance of account based CBDCs to the public. Alternatively, central banks can rely on the implied powers doctrine and wordings that allow the central bank to undertake activities incidental to the performance of its function to issue account based CBDCs.

3.4.3. Centralised and decentralised CBDCs

A CBDC can either be implemented through the centralised on decentralised ledger. Digital currency systems maintain a global state that contains all the balances of their users. Transactions comprise of updates to these systems and such transactions are serialised in a single ledger.[93] The centralised ledger is one of the most straightforward ways to implement a CBDC ledger infrastructure. On the other hand, the decentralised approach which adopts blockchain can also be used. A decentralised CBDC would be under a centralised monetary control, however, anybody can join and operate the system. This is known as a permissionless approach. There are benefits of a decentralised approach including the prevention of monetary controls and transaction censorship. Essentially, the different operators

[91] Ibid.
[92] Ibid.
[93] Sarah Allen (n 29) at 14.

are not subject to the decision of a central entity.[94] If the CBDC to be issued in the EAC aims to have the qualities of cash, then the decentralised approach is suitable because, like cash, which is not quite monitorable, it is important that operators are not subject to the decision of any central entity.

3.5. CBDCs and other Concepts – Legal Issues

3.5.1. CBDC and dispute resolution

(a) Governing law and governing jurisdiction

As the EAC contemplates issuing CBDCs, consideration must be given to the governing law. Given the fact that there are several countries in the EAC Community, it is likely that there would be political considerations. Political considerations should however be minimised to ensure that consumer trust is not eroded because of fear of control. There are suggestions that global commercial laws such as UNCITRAL Model Laws, New York, or English law[95] which normally govern laws for financial trading contracts, may be suitable. However, such suggestions are with respect to country specific CBDCs. For regional CBDCs, already established regional laws could also work. The primary consideration is that such law should be neutral, and constantly evolving to meet parties' need and the ever-changing technology landscape.

Usually, the choice of governing jurisdiction is informed by the choice of governing laws. Suggestions may be that for account based CBDCs, property laws of the EAC will apply to transfers in a manner recognised in the specific jurisdiction of the intermediary where the seller's account is located. In cases of insolvency, the bankrupt party's domestic jurisdiction will be responsible for sorting out assets. The primary point will be to examine ownership interests as recorded in such CBDC accounts, governed by the legal system governing the account.[96]

3.5.2. Legal aspects of data protection and privacy in relation to CBDCs

There are many entities with varying degrees of visibility CBDC transactions, for example, payer's bank, government institutions and the general public. With CBDCs where there is any exposure of the private keys and identification of the CBDC user, the user's private information will be exposed. There are two implications of this exposure of the user's privacy and the loss of the user's property rights – essentially, any hacker will take ownership of the user's digital money.

From a public interest perspective, the EAC needs to consider how retail CBDCs will affect data governance. Standards and rules that foster good data

[94] Sarah Allen (n 30) at 23.
[95] Barnabas Reynolds and Donna Parisi, 'The missing legal framework for central bank digital currencies' (*Reuters.com*, 19 October 2021) < https://www.reuters.com/legal/transactional/missing-legal-framework-central-bank-digital-currencies-2021-10-19/ > accessed 4 August 2022
[96] Ibid.

governance are important in establishing and maintaining open markets and a competitive level playing field, which can bring about significant economic benefits.[97] The EAC should strive to design a CBDC that balances anonymity and registration of users using their real names.

This is because the level of acceptance and usage of CBDCs depend in part on how much users trust the level of privacy offered by the CBDC. An important consideration when drafting privacy regulations for CBDC is also to understand that privacy rules are not binary. Privacy rules are on a spectrum and can be tailored according to each jurisdiction's needs and priorities. Thus, in drafting privacy rules of a CBDC in the Community, there must be a consideration of the context of the disclosure regime and policies of common laws of the EAC.[98] The EAC can explore varying degrees of privacy. It is possible to allow the legal identity of CBDC users to be unverified when they access services thus any ensuing transaction would be essentially anonymous.

There could also be options like Europe, where regulations do not allow anonymity in electronic payments, only for banknotes and coins.[99] Despite the validity of these concerns, issues such as the legal obligations related to money laundering and terrorist financing, it is important to know who is transferring what and to whom it is being transferred to. It will also be important to limit the scope of CBDC users to avoid excessive capital flows or the use of CBDCs as a form of investment.

Various privacy design choices can be explored when issuing CBDCs in the EAC. There can be privacy on a need-to-know basis which provides some level of physical separation users and the central bank where only the transactors themselves receive the data for that transaction. This is the approach adopted in designing Riskbank's e-Krona pilot model on Corda. It ensures privacy and confidentiality. Another design choice is controlled anonymity where transactions remain private to outsiders do not have access. China's digital currency e-payment adopts this approach where it is just the people's bank of China that can trace DC/EP movements.[100]

The implication of all of these is that the EAC needs to ensure that in designing a CBDC, they are complying with their data privacy laws. Government and central banks need to consider whether, in the event of a breach, they can infringe on people's privacy rights when exercising authority over CBDCs. The EAC must therefore examine its laws to determine that in certain cases there are legal controls in place to prevent the government from surveillance that violates the rights of citizens.

In terms of policy and regulatory considerations around privacy, consumers in EAC would be naturally concerned about whom they entrust their data to and how such data is used. Many would be wary about how government use their data and whether it is used at all for their benefit. Just a minority of citizens trust their own

[97] BIS Foundational Principles (n 20).

[98] World Economic Forum, 'Privacy and Confidentiality Options for Central Bank Digital Currencies Paper' in 'Digital Currency Governance Consortium White Paper Series' (n ovember 2021) <https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf > accessed 7 August 2022 at 155-174.

[99] ESCB Legal Conference 2020 (n 21).

[100] WEF 2021 (n 98) at 159.

national governments with their data.[101] If there are low levels of trust in the EAC as a regional organisation, it will result in low adoption levels of CBDCs in Africa. Thus, for EAC citizens to successfully adopt the CBDC, the regional authority must be trusted to a certain extent by citizens. Policies and regulations which foster user trust in how data is gathered are therefore essential in building trust.[102]

The EAC in issuing a CBDC must consider the three core principles in safeguarding the privacy of data:[103]

- Prioritise the best interests of citizens, especially the vulnerable population when collecting data.
- Limit the collection of personal identifiable information to what is necessary.
- Use data only for the purpose for which it was provided.

Whilst privacy and security are different concepts, data loss prevention is also important. As a result of the centralised nature of CBDCs any data loss can be monumental. This means that the EAC must ensure that current and future infrastructure is highly resilient to cyber threats and capable of providing high level protection from cyber-attacks. Adequate preparation also must be made by the community in order to ensure that where there are attacks, recovery is quick and data integrity is protected.

3.5.3. CBDC and Know Your Customer (KYC)

The EAC should consider how the CBDCs will interact with KYC procedures. In dealing with identity verification requirements some issues may arise with respect to CBDCs, depending on the model of a chosen CBDC, whether retail or wholesale. As discussed above, retail CBDCs involve the holding of private accounts at central banks. For a CBDC to achieve maximum usefulness, ordinary individuals must hold and use the CBDC. This makes it critical to understand who would manage the account and be responsible for KYC procedures since traditionally central banks do not maintain accounts for or enter business relationships with individuals, only with banks. It would be new business for central banks to allow individuals open and use CBDC accounts directly with central banks. This would bring account and identity management challenges as well as potential risks.[104]

In these situations where individuals hold accounts with the central banks (retail CBDCs), intermediaries like financial institutions and commercial banks would no longer be necessary since onboarding and KYC would be the responsibility of the central bank. This scenario would require the central banks to perform KYC checks

[101] Ipsos-World Economic Forum Project, 'Global Citizens & Data Privacy' (*Ipsos.com*, 2019) <https://www.ipsos.com/sites/default/files/global-citizens-data-privacy.pdf > accessed 5 August 2022.
[102] WEF 2021 (n 98) at 159.
[103] World Economic Forum, 'Presidio Principles: Foundational Values for a Decentralized Future' (2020) <https://www3.weforum.org/docs/WEF_Presidio_Principles_2020.pdf > accessed 6 August 2022 and Principles for digital development, 'Principle 8: Address Privacy & Security' (digitalprinciples.org) <https://digitalprinciples.org/resource/principle-8-address-privacy-security/ > accessed 6 August 2022
[104] Sarah Allen (n 30) at 24.

and Anti-Money Laundering ("AML") monitoring of their account holders directly. Whereas with wholesale CBDCs, the banks can act as intermediaries between the central banks and the CBDC users, hybrid CBDCs will also allow banks to undertake KYC considering that it is a mixture of wholesale CBDC and synthetic CBDC.

A critical question that the EAC needs to investigate is how platform users would remain anonymous without increasing the risk of money laundering? Certain options have been suggested including a scenario where users use the platform anonymously with counterparts in their day-to-day transactions. Those operators acting as intermediaries would daily submit this data to the central bank as soon as necessary whilst performing the necessary AML/KYC duties. Such a platform envisaged ought to be structured with the central bank, commercial banks/fintech and end-users separate.[105] It will be the commercial banks and fintechs that will provide all necessary consumer-facing payment services and KYC, fraud management and anti-money laundering checks. The central bank will then provide a base level of functionality for CBDC payments.[106]

Part of the risks attendant with CBDCs is financial crime. Digital currencies may enable users to undertake transactions speedily without a central authority thus, creating a platform for criminals to exchange funds across borders much faster and easily than cash. In a permissionless CBDC infrastructure, transactors can create numerous anonymous wallets and series of transactions to evade regulations that focus on large transactions.[107]

The EAC in issuing a regional CBDC will need to consider whether its legal frameworks and regulatory policies are equipped to deal with these issues or whether it will require amendments. Amendments are particularly difficult in certain African countries because of lack of expertise in such topics, legislative lethargy amongst other factors.

3.5.4. CBDCs, EAC and the Pan-African Payment and Settlement System

In September 2021, the African Export-Import Bank (Afreximbank) and AfCFTA Secretariat announced the operational roll-out of the Pan-African Payment and Settlement System (PAPSS). PAPSS is a centralised payment and settlement infrastructure built to enable instant, cross-border payments in local currencies between African AfCFTA member nations.[108] PAPPS will be a continent-wide platform for the processing, clearing, and settling of intra-African trade and commerce payments, leveraging a multilateral net settlement system.[109] For payment facilitators including banks and fintech ventures, PAPPS will enable

[105] Deloitte, 'Are Central Bank Digital Currencies (CBDCs) the Money of Tomorrow?' Deloitte, 2020 https://www2.deloitte.com/lu/en/pages/banking-and-securities/articles/central-bank-digital-currencies-money-tomorrow.html> accessed 6 August 2022 at 18.
[106] Ibid.
[107] World Economic Forum, Regulatory and Policy Gaps and Inconsistencies of Digital Currencies' in 'Digital Currency Governance Consortium White Paper Series' (n ovember 2021) <https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf > accessed 7 August 2022 at 46.
[108] Richie Santosdia, 'Overview of The Pan-African Payment and Settlement System PAPSS' (*The Fintech Times*, 25 June 2022) https://thefintechtimes.com/overview-of-the-pan-african-payment-and-settlement-system-papss/ accessed 9 September 2022.
[109] Ibid.

them to make instant and safe payment on behalf of their customers.[110] PAPPS is an infrastructure that enables payment to be initiated and settled in the local currencies of initiators and beneficiaries, removing the need for hard currencies.

The EAC has its own East African Payments System (EAPS) launched in May 2014 which functions in a similar way to the PAPPS, to enhance regional currency convertibility. In 2019 due to Kenya's dominance and other operational reasons, EAC central banks started exploring 'ways of transforming the system by linking it with other payment solutions in Africa to enable seamless transfer of cash across the continent at both retail and wholesale levels'.[111] It may be possible that in light of the AfCFTA, the EAC would consider integrating its payment system with the PAPPS.

A key consideration would be whether the current payment systems, both the EAPS and PAPPS can accommodate digital currencies. This would be worth exploring as digital currencies continue to gain traction.

4. CONCLUSIONS AND RECOMMENDATIONS

4.1. Conclusion

The potential benefits of CBDCs have resulted in the burgeoning research and interests by central banks of different countries and regional bodies. For the EAC, CBDCs can help to deal with Partner States' reluctance to trade in each other's currency. However, the benefits of CBDCs are not limited to providing a neutral currency for the EAC. CBDCs can make digital payment services universal and instantaneous. CBDCs can also manage the declining usage of cash and encourage the digitalisation of the EAC. This is a significant benefit, given the evolving digital landscape. Despite the benefits of CBDCs, there are costs such as cyber threats and loss of privacy. CBDCs can amplify already existent threats in the financial system.

In considering whether to issue a CBDC, certain conditions must be in place to assure and allay consumers' fears of many unknown risks. Although these conditions need not be in place at the early stages of issuing the CBDC, it is suggested that there must be ongoing plans to address issues as soon as possible.

With the advent of the EAMI, the precursor to the region's central bank, this is the time to draft a sound legal framework with provisions that authorise the EAMI to issue a digital currency and laws and policies that will ensure adequate safety measures.

4.2. Recommendations

- A CBDC designed for the EAC, should keep up to date with the evolving technology landscape so that it can be current enough to address the needs of the EAC market. Such CBDC must also be flexible and can adapt over time as user requirements and behaviour can change. Any CBDC must be usable, convenient, fast, cost-efficient, and programmable. It is

[110] Mike Ogbalu III, 'Boosting the AfCFTA: The Role of the Pan-African Payment and Settlement System' (Brookings: Africa in Focus, 11 February 2022) https://www.brookings.edu/blog/africa-in-focus/2022/02/11/boosting-the-afcfta-the-role-of-the-pan-african-payment-and-settlement-system/amp/ accessed 9 September 2022.
[111] Anyanzwa (n 24).

recommended that such CBDC must be interoperable with private payment solutions and available through front-end solutions throughout the EAC region.

- A critical requirement of issuing a CBDC in Africa is ensuring that it is available offline and that any dependencies, for example electricity for mobile devices, are available so as to minimise the digital divide.
- Any digital banknote in the EAC must be cheap to use, with low transaction costs much like physical cash, efficient in the sense that it allows fast payments, risk-free. In terms of consumer protection, it must have high fraud prevention and be easy to use for businesspeople and unskilled people. The EAC needs to work together with internet service providers to build affordable internet infrastructure.
- Financial literacy and capacity building of citizens of the EAC would be necessary to enable acceptance and usability.
- The EAMI should at this stage, recruit and build adequate legal capacity in their legal department to have legal assessments of CBDCs as the issues arise.
- To deal with cyber risk, the EAMI in drafting CBDC regulation, could criminalise unauthorised retrieval of personal information of CBDC account owners making such information confidential.

THE POTENTIAL OF BLOCKCHAIN TECHNOLOGY IN FACILITATING INTRA-AFRICAN TRADE: THE CASE OF DIGITAL SINGLE WINDOWS

Chidochashe Ncube*

ABSTRACT

The concept of a Single Window for trade was introduced in the 1980s in Singapore and Sweden to reduce border clearance time from four days to approximately 15 minutes. As a result, Single Windows gained global traction as trade facilitation tools. Single Windows can be defined as facilities that allow parties involved in trade and transport to lodge standardised information and documents using a single-entry point to fulfil all import, export, and transit-related regulatory requirements. Although these Single Windows have registered several notable positive results, there have some pain points that are slowly overtaking the benefits and these relate to interoperability, concerns on data trustworthiness and the persistence of paper. With regards to interoperability, most national single windows in Africa are fragmented and as a result, it is difficult to seamlessly exchange customs data which makes it extremely difficult for customs to detect anomalies in the submitted data. Digital technologies particularly blockchains have the potential to further improve Single Windows. Blockchain technology has features that could potentially revolutionise customs administration and border clearances. Studies suggest that blockchain can improve the ability for different stakeholders to interoperate by sharing real time and immutable data with 360-degree visibility of transactions.

* Legal Manager, Zimbabwean Investment & Development Agency | Ph.D Cand., *University of the Western Cape.*

INTRODUCTION

Trade costs are inarguably one of the major barriers to trade. Conversations on trade facilitation are influenced by the desire to significantly lower trade costs for businesses to enable them to reap the full benefits of cross-border trade. A significant share of these trade costs results from the time and money spent on paperwork and multiple submissions of the same information as required by various government agencies to release goods for export and allow them to enter the importing country.[1] When the Single Window for trade was conceptualised, it was to try and reduce the processing time of submitted documentation by traders. From the time the concept was introduced to present day, Single Windows have acted as a single-entry point within which traders are able to fulfil all import, export and transit-related regulatory requirements thus reducing clearance time. Evidence from case studies referred to in this paper shows that Single Windows have managed to significantly reduced trade costs and halve document processing time.[2]

African countries such as Kenya, Egypt and Mauritius that have implemented Single Windows for trade have constantly ranked higher on trade facilitation according to the statistics provided by the Trade Facilitation Indicator developed by the Organisation of Economic Co-operation for Development (OECD).[3] Although these Single Windows have registered several notable positive results, there have some pain points that are slowly overtaking the benefits and these relate to interoperability, concerns on data trustworthiness and the persistence of paper. With regards to interoperability, most Single Windows in Africa are fragmented and as a result, it is difficult to seamlessly exchange customs data. Often, traders are expected to enter the same data more than once and this has been exacerbated by the accelerated adoption of digital technologies.

The current architecture of Single Windows is likely to pose challenges for the full operationalisation of the African Continental Free Trade Area (AfCFTA). The preferential trade framework is expected to significantly increase intra-African trade volumes. The projected increase in intra-African trade requires enhanced trade facilitation measures particularly at border posts for faster clearance of goods. Hence, there is an inherent need to fully improve the Single Windows for better interoperability, faster clearance of goods and harmonisation of trade data.

This paper aims to unpack the extent to which blockchain technology can be used to improve the Single Windows in Africa for better trade facilitation. Blockchain technology which was first developed to underpin cryptocurrencies has features that could potentially revolutionise customs administration and border

[1] World Economic Forum, *Window of Opportunity: Facilitating Trade with Blockchain Technology* (White Paper, 2019) https://www.weforum.org/whitepapers/windows-of-opportunity-facilitating-trade-with-blockchain-technology (accessed 4 May 2022) 4.

[2] See section 2.3 for case studies in Africa on the Single Window for trade.

[3] After the entry into force of the Trade Facilitation Agreement of the World Trade Organisation, the Organisation of Economic Co-operation and Development (OECD) developed trade facilitation indicators that have been used to rank countries on various trade facilitation measures. For the period 2017 to 2019, Mauritius, Kenya and Egypt have been consistently ranking higher. For more information refer to https://www.oecd.org/regreform/facilitation/indicators.htm (accessed 31 August 2022).

clearances. Blockchain can improve the ability for different stakeholders to interoperate by sharing real time and immutable data with 360-degree visibility of transactions. The main question to be answered therefore is to what extent can blockchain revolutionise trade facilitation through the full digitalisation of Single Windows in Africa? Reference will be made to a few case studies and pilot projects for electronic customs using blockchain technology. The purpose will be to extrapolate useful lessons for African countries to enhance intra-African trade through trade facilitation.

2. THE SINGLE WINDOW CONCEPT

Globalisation and economic liberalisation have continuously transformed international trade into a world without borders characterised by free movement of goods, capital and persons.[4] Subsequently, customs have been facing difficulties with managing cross-border transactions using traditional means due to the complexities associated with collecting, managing, interpreting and using voluminous data.[5] Over the past decades, the adoption of Information and Communication Technologies (ICTs) in customs has greatly contributed to customs modernisation by simplifying procedures, improving transparency, diminishing corruption and reducing time and costs.[6] The Single Window was one of the first electronic tool to modernise customs. Single Windows were first introduced in the late 1980s in Sweden and Singapore and have since become a centrepiece of trade facilitation efforts around the world.[7]

In many countries, businesses involved in international trade have regularly had to prepare and submit large volumes of information and documents to governmental authorities to comply with import, export and transit-related regulatory requirements.[8] In the past, this information once gathered would then have to be submitted to different governmental agencies, each with each own documentation forms and systems which were either manual or automated. The process of complying with these regulatory requirements together with associated compliance costs constituted a serious burden to both governments and the businesses and became a serious barrier to the development of international trade.[9] For this reason, development institutions and research think-tanks started building a case for the development of Single Windows and other ICT tools for better trade facilitation.

[4] Dejong M Johnson M & Pandey P 'Interagency cooperation: Focused on but not limited to Customs-Tax Cooperation' in World Customs Organisation' (2018) 111, World Customs Study on illicit Trade'.

[5] Ntuli F, 'Trade Security Role of Customs Administrations within the AfCFTA' (*Afronomics Law Blog* 18 March 2021) https://www.afronomicslaw.org/category/analysis/trade-security-role-customs-administrations-within-afcfta (accessed 5 June 2022).

[6] Mujica S, 'E-cooperation: Information Technologies that may allow for exchange information between national and international entities.' Chile Case Study Topic 1.3 (2012) 142 World Customs Organisation Study Topic 1.3.

[7] World Economic Forum (n 1) 5.

[8] United Nations Economic Commission for Europe Recommendation no. 33 of 2004 ECE/TRADE/352.

[9] Ibid.

2.1. Definition of Single Windows

The definition of a Single Window is expressed in the United Nations Economic Commission for Europe (UNECE) Recommendation 33 of 2004.[10] The recommendations define a single window as:

> [A] facility that allows parties involved in trade and transport to lodge standardised information and documents with a single-entry point to fulfil all import, export, and transit related regulatory requirements. If information is electronic, then individual data elements should only be submitted once.[11]

The World Customs Organisation (WCO) expanded the definition to provide further scope on the concept of the Single Window. The WCO defined the Single Window Environment as:

> [A] cross-border intelligent facility that allows parties involved in trade and transport to lodge standardised information, mainly electronic with a single-entry point to fulfil all import, export and transit-related requirement.[12]

The World Bank further tried to simply the definition of Single Windows in the Doing Business Report of 2017 as:

> [A] system that receives trade-related information and disseminates it to all relevant governmental authorities, thus systematically conducting controls throughout trade processes.[13]

From the definitions above, what is clear is that a Single Window is a single point of entry that allows traders to submit documents electronically. The core function of a Single Window is to expediate and simplify information flows between traders and government agencies and bring meaningful gains to all parties involved in cross-border trade.[14]

Single windows were designed to halve document processing time at border posts and increase compliance with customs procedures through the use of a single entry point for information submission.[15] The first Single Window introduced in Sweden managed to reduce clearance time from 4 days to 15 minutes.[16] From then, Single Windows became an important tool for trade facilitation around the world.[17]

---

[10] Ibid
[11] Ibid.
[12] Mujica S (n 6) 150.
[13] World Bank, Doing Business Report (2017 Report) https://archive.doingbusiness.org/en/reports/global-reports/doing-business-2017 (accessed on 8 August 2022).
[14] UNECE Recommendation (n 8) 6.
[15] UNECEE Recommendation no. 33 of 2004.
[16] World Economic Forum (2019) 5; African Alliance for E-commerce 'Assessing Single Window Performance: an overview of the peer review exercise undertaken in five countries' (*World Customs Organisation News (n d))* https://mag.wcoomd.org/magazine/wco-news-81/assessing-single-window-performance-an-overview-of-the-peer-review-exercise-undertaken-in-five-african-countries/ (accessed 14 July 2022).
[17] World Economic Forum (n 1) 5.

The Single Window as an information system, facilitates the exchange of information between the various parties involved in the supply chain process, and greatly contributes to border agency cooperation thus speeding up the movement of goods across borders.[18] Typically, Single Windows bring together dozens of government agencies in charge of areas such as health, quarantine, immigration and technical standards allowing traders to submit all documents required through the singular window.[19]

2.2. The Legal Basis for the Application of Single Windows in Customs Administration

The adoption and maintenance of Single Windows in Africa materialises in the World Trade Organisation Agreement on Trade Facilitation (TFA)[20]and the Protocol on Trade in Goods of the Agreement Establishing the African Continental Free Trade Area. The provisions of these Agreements shall be fully unpacked below.

2.2.1. Agreement on Trade Facilitation

In 2001, the Ministerial Council of the World Trade Organisation (WTO) passed a declaration to commence the Doha Round of Negotiations that were to focus on several trade related issues including trade facilitation. Trade facilitation negotiations at WTO were focused on how procedures and controls governing the movement of goods across national borders could be improved to reduce associated cost burdens and maximise efficiency while safeguarding legitimate regulatory objectives.[21] The objectives of the TFA include expediting the movement, release and clearance of goods as well as improving cooperation between customs and other government agencies.[22]

To achieve the said objectives, the TFA encourages countries to adopt or maintain electronic single windows for trade facilitation.[23] Article 10.4.1 of the Agreement indicates that a single window enables traders to submit documentation and/or data requirements for importation, exportation, or transit of goods through a single-entry point to the participating authorities or agencies.[24] For African countries, the commitment to maintain Single Windows did not end with the coming into force of the Trade Facilitation Agreement at WTO level. The Agreement Establishing the African Continental Free Trade Area also provides the

[18] Mbouwé WD 'Digital Solutions for trade facilitation' (*Tralac blog* 1 July 2020) https://www.tralac.org/blog/article/14716-digital-solutions-for-trade-facilitation.html (accessed 14 July 2022).
[19] World Economic Forum (n 1) 5.
[20] Annex to the Protocol amending the Marrakesh Agreement establishing the World Trade Organisation: Agreement on Trade Facilitation 2017. The full text is available at https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/940.pdf&Open=True (accessed 15 July 2022).
[21] United Nations Economic and Social Commission for Western Asia (2011) 'Key Factors in Establishing Single Windows for Handling Import/Export Procedures and Formalities: Trade Facilitation and Single Windows" (*United Nations Economic and Social Commission for Western Asia, July 2011*) 18.
[22] The Preamble of the Agreement on Trade Facilitation, 2017.
[23] World Economic Forum (n 1) 6.
[24] Article 10.4.1 Agreement on Trade Facilitation 2017.

basis for and maintaining Single Windows.

2.2.2. AfCFTA Framework on Single Windows

The establishment of the AfCFTA[25] created a single market for Africans with the free movement of goods, services and persons. Dubbed the largest free trade area, the AfCFTA intends to boost intra-African trade through the removal of both tariffs and Non-Tariff Barriers to trade.[26]

It is important to note that the success or effectiveness of trade liberalisation under the AfCFTA is largely dependent on how trade is facilitated within the free trade area.[27] The International Monetary Fund (IMF) projects that the benefits of the AfCFTA will increase four-fold through trade facilitation measures.[28] Similarly, the United National Economic Commission for Africa (UNECA) projects that intra-African trade will double through enhanced trade facilitation.[29] Article 4 of the Agreement Establishing the AfCFTA recognises the importance of enhancing trade facilitation in realising the objectives of the AfCFTA.[30]

The AfCFTA framework provides for specific undertakings on trade facilitation, and these are contained in the Annexes to the Protocol on Trade in Goods. The Protocol on Trade in Goods has three Annexes that specifically focus on trade facilitation at national borders namely: Annex 3 on Customs Cooperation and Mutual Administrative Assistance, Annex 4 on Trade Facilitation and Annex 8 on Transit. Of particular importance to Single Window initiatives is Annex 4 which defines a Single Window as:

> [A] facility that allows parties involved in trade and transport to lodge standardised information and documents with a single-entry point to fulfil all import, export and transit-related regulatory requirements, and in the case of electronic information, the single submission of individual data elements.[31]

Annex 4 goes further to encourage State Parties to establish and maintain Single

[25] The AfCFTA was successfully launched into an operational phase at the 12th Extraordinary Summit of the African Union on 7 July 2019. https://au-afcfta.org/ (accessed on 7 August 2022).

[26] World Bank, 'The African Continental Free Trade Area (World Bank, (n d) https://www.worldbank.org/en/topic/trade/publication/the-african-continental-free-trade-area (accessed on 7 August 2022.

[27] Sithole L, 'The Role of Trade Facilitation in Addressing Non-Tariff Barriers in the African Continental Free Trade Area' (*Afronomics Law Blog, 28 March 2021*) https://www.afronomicslaw.org/category/analysis/role-trade-facilitation-addressing-non-tariff-barriers-african-continental-free#:~:text=The%20AfCFTA%20Agreement%20provides%20a%20legal%20framework%20with,mechanisms%20other%20than%20the%20imposition%20of%20tariffs%20%28NTBs%29. (accessed on 12 July 2022).

[28] Abrego L, Amado MA, Gursoy T, Nicholls GP and Perez-Saiz H 'The African Continental Free Trade Agreement: Welfare Gains Estimates from a General Equilibrium Model' 2019, International Monetary Fund Working Paper, https://www.imf.org/en/Publications/WP/Issues/2019/06/07/The-African-Continental-Free-Trade-Agreement-Welfare-Gains-Estimates-from-a-General-46881. (accessed on 10 July 2022).

[29] Sithole L (n 27).

[30] Article 4, of the Agreement Establishing the African Continental Free Trade Area.

[31] Article 1 of Annex 4 to the Protocol on Trade in Goods of the Agreement Establishing the African Continental Free Trade Area.

Windows, to enable traders to submit documentation and/or data requirements for importation, exportation, or transit of goods through a single-entry point to the participating national authorities.[32] In addition, where documentation and / or data requirements have already been fulfilled through the Single Window, the same documentation and / or data requirements shall not be required by national authorities except in urgent circumstances and other limited exceptions which are made public.[33] Under the AfCFTA framework, State Parties that maintain Single Windows are expected to notify the AfCFTA Secretariat of the operation details of those Single Windows.

2.3. Implementation of Single Windows in Africa and their Impacts in Border Processes

African countries have not been left behind in the quest to facilitate trade through the adoption of Single Windows. The development of Single Windows in Africa has continued to be achieved through the assistance of development partners under the auspices of preferential trade agreements. The following section focuses on the impact of Single Windows in border processes for selected African countries. The countries referred to were simply chosen based on the availability of data on Single Windows.

2.3.1. Digital payments of customs duties and fees

One of the functions of Single Windows in Africa has been to reduce invoicing by automating the computation of duties and fees, thereby reducing corruption in customs and time for traders to make payments.[34] Digitalised payment systems translate into accelerated reconciliation of amounts to be paid to government agencies and this in turn speeds up the clearance time for goods. In DRC, Togo and Benin, for instance, traders receive a single invoice where all costs at the port such as terminal handling charges, regulatory duties and taxes are combined into a single invoice that is automatically sent to the importer or relevant party.[35] Once the amount reflected on the electronic invoice is paid in full by the trader, the trader's bank then settles amounts for every stakeholder involved and goods are released. This has managed to significantly reduce the time that is taken between the issuance of invoices, settlement and release of goods. The government of Tanzania adopted a Single Window with digitalised payment systems. The digitalisation of customs clearance and duties managed to cut import clearance time from 9 days to less than a day.[36]

[32] Article 18 of Annex 4 to the Protocol on Trade in Goods of the Agreement Establishing the African Continental Free Trade Area.
[33] Ibid.
[34] World Economic Forum (n 1)6.
[35] Ibid.
[36] Ibid.

2.3.2. Digital single-entry points for documentation

At the core of adopting Single Windows is the desire to enable traders to submit all documentary requirements through one entry point, typically electronic, to improve compliance and facilitate trade. The adoption of Single Windows assist agencies in processing the submitted documents faster thereby accelerating clearance at border posts. Kenya has a digital Single Window which is mainly focused at improving trade compliance by enabling traders to submit all documents required for border clearance electronically.[37] As result, the average time spent in processing applications in Kenya dropped by 50%, the number of documents required for processing halved and traders saved enormous amounts of time previously spent visiting different agencies.[38] In Cameroon, after the adoption of the digital single point of entry, the time to import used vehicles fell from 7 days to 2 days, the time to lodge shipping manifests from 7 days to a day and the time to obtain import licences from 8 hours to 15 minutes.[39]

Also, the Single Window in Mauritius allows for the submission of customs declarations, their processing and return by electronic means through TradeNet, a proprietary system that allows the electronic transmission of documents between various parties involved in the movement of goods.[40] It is estimated that the system has decreased the average clearance time of goods from 4 hours to 15minutes with an estimated savings of around 1% of Mauritius's Gross Domestic Product.[41]

Single Windows have not only managed to reduce the re-entry of the same information to multiple agencies but has also improved the legibility of trade documents that were traditionally completed by hand thereby reducing the risk of errors.[42] These benefits have contributed to why the Single Window has gained a lot of traction. Currently, with the assistance of the European Union, African countries that are members of the Common Market for Eastern and Southern Africa (COMESA) are upgrading border infrastructure including Single Windows and the electronic certificates of origin for better customs cooperation.[43] The Euros 6, 8 million border project which will run for two years is going to upgrade facilities in Zambia, Zimbabwe, Malawi and Tanzania.[44] This facility is meant to support the full operationalisation of the AfCFTA through enhanced trade facilitation at border posts.

[37] https://www.slideshare.net/Africanalliance/implementation-of-the-kenya-national-single-window-systemkentradeswc2016 (accessed on 10 July 2022).
[38] World Economic Forum (n 1)6.
[39] https://www.slideshare.net/Africanalliance/the-single-form-for-foreign-trade-operators-guce-gie-cameroon (accessed on 10 July 2022).
[40] UNECE Recommendation Number 33 (n 6).
[41] Ibid.
[42] World Economic Forum (n 1) 7.
[43] Kazunga O 'East Africa: COMESA begins Euros 6.8 million Border Upgrade Projects' (*The Herald: All Africa* 11 March 2021) https://allafrica.com/stories/202103110178.html (accessed 15 June 2022).
[44] Ibid.

2.4. Single Window Pain Points

Although single windows have many benefits, in most African countries they have not been implemented in full and they suffer from a number of pain points that hinder them from reaching their fullest potential in facilitating trade. The challenges that Single Windows face include lack of interoperability, concerns on data trustworthiness and the persistence of paper. Although there are quite a few challenges, for the purpose of this paper, analysis shall be limited to the identified challenges.

2.4.1. Interoperability

Interoperability can be defined as the ability of two or more systems to exchange and use information across borders without additional effort on the part of the end user.[45] In making a case for Single Window interoperability, UNECE identified the following as drivers for interoperability:

- Regional integration for the simplification, modernisation and harmonisation of export and import procedures;
- Trade facilitation to allow all economic operators including small and medium sized enterprises to comply with regulatory requirements to improve competitiveness in a global market; and
- Effective risk analysis to combat illicit activities by traders such as trade-based money laundering.[46]

Single Windows in Africa do not interoperate in that they cannot facilitate for real-time cross-border exchange of information. This is mainly because of disparate national databases, lack of platforms for efficient exchange of cross-border data and differences in document formats.[47] The existing Single Windows are unable of allowing for the seamless exchange of customs data across the border and as a result, the trader is expected to submit the same information at every entry point. As result, it becomes time consuming and costly for the trader and difficult for border agencies to conduct effective risk analysis. The result is customs control agencies that work in exporting countries, importing countries and transit countries end up operating with isolated data. As a result, there is need to ensure that Single Window fully interoperate to achieve the identified objectives, regional integration, trade facilitation and effective risk management.

2.4.2. Trustworthiness and security of data submitted

As already stated above, due to lack of interoperability, traders often must re-submit the same data multiple times to different agencies. That exercise tends to undermine the trustworthiness of the data in a Single Window.[48] The data that is entered is prone to tampering by employees of border agencies and that extremely

[45] United Nations Economic Commission for Europe Recommendation Number 36 of 2017: Single Window Interoperability, UNECE/TRADE/431.
[46] Ibid.
[47] World Economic Forum (n 1) 7.
[48] World Economic Forum (n 1) 10.

undermines the trustworthiness of all information. In addition, the security of Single Windows has been repeatedly questioned and companies have become reluctant to submit sensitive commercial and financial data through the Single Window.[49] This challenge is exacerbated in countries with centralised management of data but with limited cybersecurity protections and electronic signature laws.[50] The limited legal protection is especially an issue in Africa as countries seem to be lagging behind in enacting laws for cybersecurity and data protection..

In 2021, Werkmans Attorneys conducted a study on data protection laws and according to their findings, approximately half of the 54 countries in Africa had enacted data protection and cybersecurity laws.[51] In addition, there has been delays in the operationalising and implementation of the African Union Convention on Cybersecurity and Personal Data Protection[52] which is meant to be a mechanism to address the risks from the use of electronic data and individual records. The Convention which was adopted in 2014 is yet to into force as it has not yet reached the minimum 14 ratifications required for entry into force.

2.4.3. The persistence of paper

Despite the commitments in the TFA to introduce paperless trading, some border agencies in Africa still insist for traders to file paper-based documents and visit agencies in person.[53] In some cases, the persistence of paper is caused by limited government budget that makes it difficult for Single Windows to be fully operationalised. As a result, border agencies end up having to process the trade data using manual means that tend to threaten the credibility of same. A study by the World Economic Forum concluded that even in more digitised settings, updates to agencies' databases can require manual interventions that tend to waste time, increases costs and the odds of error.[54]

These challenges are likely to be exacerbated in the region once trading fully commences under the AfCFTA. The projected boost in intra-African trade suggests that there will be an increase in trade volumes. If the challenges are not addressed, the current architecture of Single Windows is likely to affect the speed at which transactions are settled within the region thus delaying the successful full implementation of the trade area. Hence, there is need to investigate other solutions that will enhance trade facilitation measures by significantly reducing the time it takes before goods are cleared.

This paper suggests the use of blockchain technology to address the challenges presented by Single Windows, to enhance trade facilitation to boost intra-African trade. The aim of this paper is not to compare blockchain technology to other digital technologies or to allege that other digital technologies cannot address the identified challenges. Rather, it seeks to assist African governments consider the

[49] Ibid.
[50] Ibid.
[51] https://www.werksmans.com/legal-updates-and-opinions/data-protection-and-privacy-regulation-a-roundup-of-developments-in-africa-in-2021/ (accessed on 31 August 2022).
[52] For the text of the Convention, https://issafrica.org/ctafrica/uploads/AU%20Convention%20on%20Cyber%20Security%20and%20Personal%20Data%20Protection.pdf (accessed on 8 August 2022).
[53] World Economic Forum (n 1) 8.
[54] Ibid.

potential use of blockchain technologies to enhance trade facilitation.

3. THE DIGITAL TECHNOLOGY REVOLUTION

The world is currently at the brink of a technological revolution that will fundamentally change the way people live, work, relate to one another and trade.[55] Dubbed the 'Fourth Industrial Revolution', the fusion of Artificial Intelligence,[56] Blockchain technology,[57] 3-D printing[58] and Internet of Things[59] is promising to reshape the world as we know it now. However, it is important to understand that these technologies they were enabled by several factors that were developed overtime. Hence, to better understand the digital technologies, it is important to first outline the developments in computing power, communication technologies and information processing.

The first industrial revolution began in the late 18th century and the technologies accompanying it began to lower transport and communication costs dramatically, triggering the massive expansion of trade, capital and technology flows.[60] The period is well known for steamships and railways that transformed transportation. Steamships lowered transportation costs overseas and railways lowered in-land transportation costs which made both regional and global economic integration a reality. In addition to transportation technologies, the telegraph was developed and it significantly lowered communication costs. The telegraph was as revolutionary in its day as the internet is now, effectively ushering in the modern era of instantaneous global communications.[61]

The second industrial revolution was powered using electric power to create mass production. Electrification improved rail designs, high-speed trains and other innovations that further reduced transportation costs.[62] Perhaps, the most celebrated innovation of this period is the container. Containers made shipping of goods easier by substantially reducing *ad valorem* transportation costs. The communication

[55] Schwab K 'The Fourth Industrial Revolution: What it means, how to respond' *(World Economic Forum*, 14 January 2016) https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab (accessed 9 June 2021).

[56] Artificial intelligence leverages computers and machines to mimic the problem solving and decision-making capabilities of the human mind. (IBM 'Artificial Intelligence' 3 June 2020) https://www.ibm.com/cloud/learn/what-is-artificial-intelligence (accessed 2 May 2022); Russell SJ & Norvig P, 'Artificial Intelligence: A modern Approach' (1995).

[57] See discussion from paragraph 3.1 on blockchain technology.

[58] 3D printing, also known as additive manufacturing is the process of making three dimensional solid objects from a digital file. It makes it possible to complex shapes using less material than traditional manufacturing processes, see 3-D Printing .com available at https://3dprinting.com/what-is-3d-printing/ (accessed on 2 May 2022); Rideout B 'Printing the Impossible Triangle: The Copyright Implications of Three-Dimensional Printing' (2012) 5 J. Bus. Entrepreneurship & L. 161.

[59] The Internet of Things (IoT) refers to the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects, see GSMA Association 'Understanding the Internet of Things' July 2014 available https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf (accessed on 2 May 2022).

[60] World Trade Organisation 'The future of world trade: How digital technologies are transforming commerce' (2018)18 World Trade Organisation Report https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf (accessed on 1 May 2022)

[61] Ibid.

[62] Schwab K (n 55)

sector also embraced a number of innovations such as satellites, fibre and optic cables that again, reduced communication costs.

Following, the world economy was further transformed using electronics and information technologies. The adoption of the internet, electronics and ICT tools commonly known as the third industrial revolution further reduced the cost of doing business. The World Trade Organisation (WTO) posits that the 19th century was marked by the falling costs of trading commodities, the 20th century was marked by the falling cost of trading in manufactured goods and the 21st century will most likely be marked by the falling cost of trading information.[63]

These developments in communications combined led to the accelerated development of digital technologies that are fused in the fourth industrial revolution.

3.1. The History Behind Blockchain Technology

The term 'blockchain' can be translated to mean a combination of blocks that are chained together. The term block denotes a number of transactional records, whether financial or non-financial which are linked altogether by the chain components equipped with a hash function with which any given data (keys) of arbitrary size can be converted into those of fixed size with another format (hashes).[64] Once created, every transaction is subject to confirmation by a group of participants in the ecosystem.[65] Then the transaction is paired up with the previous entry in a manner that ensure the consistency of all the existing data on the chain of digital blocks.[66]

The World Customs Organisation (WCO) Report of 2019 provides a more digestible definition for what blockchain technology is. It is defined as a type of sophisticated cryptographic distributed architecture with a continuously growing list of records called blocks.[67] Blockchain has the capacity to move any kind of data swiftly, securely and at the same time, make a record of transaction available instantly, in a trusted and immutable manner, to the participants in a blockchain network.[68] Blockchains employ cryptography (encryption) in each transaction update and they are verified across the network with each participant having access to the digital copy of the entire transaction record secured through encryption.[69]

The technology first appeared in 2008 with the cryptography expert community as a component of Bitcoin and for that reason, technology has widely been associated with cryptocurrency. However, blockchain is to bitcoin and other cryptocurrencies what the internet is to emails.[70] The internet is in loose terms, a

[63] World Trade Organisation (n 58) 19.
[64] Okazaki Y, 'Unveiling the potential of blockchain for customs' (2018) 6 World Customs Research Paper No. 45 of 2018.
[65] An ecosystem in terms of blockchain platforms is a category of competing participants called miners. Miners work on transactions in order to export the information into virtual blocks with limited recording capacity.
[66] Okazaki Y, (n 64) 7.
[67] World Customs Organisation (n 63) 17.
[68] Ibid.
[69] Van der Nest G, 'Distributed Ledger Technology: Opportunities for Africa's trade' (2018) 4 Tralac Trade Brief No. US18TB04/2018.
[70] Kaiserman S 'Bitcoin is to Blockchain as Email is to the Internet' (LinkedIn, 12 January 2018)

'protocol layer that enables emails[71] and likewise, blockchain is merely a network upon which cryptocurrencies are conceptualised.

Blockchain was conceptualised by an individual or group of people under the *alias* Satoshi Nakamoto in a Whitepaper for peer-to-peer electronic cash system that was published in 2008.[72] The Whitepaper proposed an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.[73] It is for this ability to transact without the need for a trusted third party that the Economist termed blockchain technology 'the trust machine.'[74]

The concept was developed to address the problem of double-spending by using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.[75] In terms of privacy, the information that is presented on the blockchain is accessible and visible to anyone with access to the network. This conceptual framework was based on the fact that the traditional banking model achieves a level of privacy by limiting access to information to the parties involved.[76] With bitcoin[77] and blockchain, there is a necessity to announce all transactions publicly. Regardless, privacy can be maintained by breaking the flow of information in another place meaning, the public can only see that there has been a transaction between parties but without access to the specific knowledge that links the transaction to anyone.[78] In essence, all authorised persons have 360-visibility of the transaction in a manner that also secures the integrity of parties involved. The immutability and time-stamping features of blockchain and bitcoin offered appealing assurances against fraud at a juncture where big players in the financial system were in the headlines for tampering with book-keeping and market metrics.[79]

In 2013, the popularity of blockchain technology grew beyond bitcoin as a result of its use in other cryptocurrencies particularly Ethereum. A 19-year-old programmer Vitalik Buterin published a Whitepaper that laid out his plan for a blockchain system that could also facilitate decentralised applications.[80] The Whitepaper conceptualised Ethereum also duped 'blockchain 2.0' which was released in 2015. Ethereum was seen as a further development of blockchain because it introduced smart contracts.[81] Smart contracts and the automation of

https://www.linkedin.com/pulse/bitcoin-blockchain-email-internet-sheri-kaiserman (accessed 7 June 2022).

[71] Ibid.

[72] Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system* (2008) 1 https://www.bitcoin.org/bitcoin.pdf (accessed 2 May 2022).

[73] Ibid.

[74] The Economist 'The Trust Machine' (*The Economist, 31 October 2015)* https://www.economist.com/leaders/2015/10/31/the-trust-machine (accessed 2 May 2022).

[75] Satoshi Nakamoto (n 72) 2.

[76] Ibid., 3.

[77] For more information on bitcoin see https://bitcoin.org/en/ (accessed 2 May 2022).

[78] Satoshi Nakamoto (n 72) 3.

[79] Ganne E 'Can Blockchain revolutionize International Trade?' (2018) World Trade Organisation.

[80] Ibid., 3.

[81] Smart contracts are computer programmes that self-execute the terms of a contract when specific conditions are met. The applications run exactly as programmed without any third-party interference or delays. See Ethereum 'Introduction to Smart Contracts' 30 October 2021, https://ethereum.org/en/developers/docs/smart-contracts/ (accessed 16 June 2022); Stuart D. Levi and Alex B. Lipton, Skadden, Arps, Slate, Meagher & Flom LLP 'An Introduction to Smart

transaction constituted a revolution within a revolution and that sparked much interest for the potential use of blockchain technology in trade.[82] Solutions such as the Corda,[83] Quorum[84] and Hyperledger Fabric[85] that are commonly used in international trade have also been developed.

Although the terms blockchain and distributed ledger technology (DLT) have sometimes been used synonymously, they mean different things. A distributed ledger is a form of database that exists across several locations or among multiple participants and blockchain technology is simply a form of a distributed ledger technology.[86] The relationship between blockchain and DLT can be contextualised more in the same way as that of Kleenex and facial tissues in that the former is a type of the latter but has become more popular that it has been ingrained in people's minds as what the product is.[87] For the purpose of this study, blockchain technology will be referred to in its stricter sense, as being a form of a DLT.[88]

3.2. Types of Blockchains

Generally, blockchains are classified as public, private or consortium, permissioned or permissionless. However, it is important to state that the definitions of these terms are not cast in stone mainly because as the technology matures, new classifications and definitions come up. The classifications are further discussed below.

3.2.1. Public versus private and consortium blockchains

The distinction between public, private and consortium blockchains is linked to the management of the platform (who manages the platform) and user authentication (level of anonymity of participants).[89] Public platforms are not controlled by any specific party, the transactions are public and participants are allowed to maintain full anonymity. Since the platforms are not controlled by anyone, participants rely on nodes to come to a consensus before any data entered can be stored on to a ledger.

In respect of private blockchains, the permission to validate and write data on

Contracts and their Potential and Inherent Limitations'26 May 2018 Havard Law School Forum on Corporate Governance, https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ (accessed 16 June 2022); Wei-Meng L *'Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript'* (1ed (2019)) Apress: New York.

[82] Ganne E (n 79) 4.

[83] For a discussion on Corda see 3.2.2 (iii) below.

[84] See para 3.2.2 (ii) below.

[85] See para 3.2.2 (i) below.

[86] Van der Nest G (n 69) 1.

[87] Insights 'Differences between Blockchain and DLTs' (*Marcopolo Network* 30 January 2018) https://www.marcopolonetwork.com/articles/distributed-ledger-technology/ (accessed 3 August 2022).

[88] For a discussion on DLTs see World Bank 'Blockchain and Distributed Ledger Technologies'12 April 2018 https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt (accessed 3 June 2022)..

[89] Ganne E (n 79) 9.

the block is controlled by one entity trusted by all the participants who are easily identifiable.[90] Transactions are verified by a restricted number of nodes according to the rules of the blockchain and that allows for greater efficiency and even much faster processing of transactions than public blockchains.[91] In addition, because participants are known, it is easier for human intervention to fix faulty nodes using very little computing power as compared to public blockchains. As already indicated, private platforms are controlled by a single entity hence they are more centralised as compared to public platforms that are highly decentralised.

Consortium blockchains are a special type of private blockchains that operate under the oversight of a group of entities. Instead of having a single entity that controls the platform, consortiums are designed in a way that they can be controlled by a group of entities each of which operates a device connected to the platform.[92] They have a hybrid system in that instead of letting anyone with internet connection participate in the transaction verification process (like in public networks), or letting a single entity have full control (like in private networks), a few selected nodes are predetermined to control the consensus process.[93]

Public blockchains are considered more secure and resistant to malicious attacks because they are decentralised, but they often fail on scalability which makes them a less viable option for the international trade system. As a result, developers, governments and companies have identified consortium platforms as a viable option and have started implementing the programmes for many different uses. The Hyperledger Fabric is the most common consortium blockchain that is being used by institutions. For instance, the WCO started exploring the use of the technology in the customs domain primarily in fraud detection, misuse of blockchains including cryptocurrencies for illicit trade, evasion of duties and taxes, intellectual property violations, money laundering and other financial crimes.[94]

3.2.2. Permissioned *vs.* permissionless blockchains

The distinction between permissioned and permissionless blockchains relates to the extent at which access to the platform is restricted. With a permissioned blockchain, access is restricted at various levels on the specificities of the platform. On the other hand, permissionless blockchains are open to anyone with a computer and there are no restrictions imposed on who can access the platform or validate transactions.[95] When Satoshi Nakamoto conceptualised bitcoin and blockchain technology, the idea was for the platform to be a permissionless public blockchain that is accessible to anyone with a computer. However, when developers and businesses started noting the potential use of blockchain technology in other spheres of life, majority of them started favouring permissioned networks more because of their enhanced level of control and privacy. Many blockchain platforms in international trade, as will be noted later are permissioned consortium networks.

The challenges with using permissionless public blockchain platforms for

[90] Ganne E (n 79) 10; World Trade Organisation (n 58) 17.
[91] Ibid., 10.
[92] Ibid., 11.
[93] Ibid., 11.
[94] World Customs Organisation (n 63) 10.
[95] Ganne E (n 79) 11.

customs administration manifest from the fact that users are allowed to be anonymous. This becomes quite problematic considering that in international trade, parties to transactions, the value of goods being imported or exported, the nature of goods to be exported or imported should be disclosed. Full disclosure will then help customs administrations conduct adequate checks and verification processes. For that reason, customs administrations should consider using platforms that afford them some degree of control such as in the case of private or consortium permissioned platforms.

There are mainly three types of blockchain infrastructure that have been developed overtime to be used beyond cryptocurrencies or financial services. These solutions are permissioned and they were conceptualised based on the possible pitfalls of using public permissionless platforms for businesses. There are as follows:

(b) Hyperledger Fabric

The Hyperledger Fabric is an open-source blockchain that facilitates a multi-channel global broadcast infrastructure in which peers are able to interact with one another through a series of channels.[96] The channels can either include all of the peers on the networks or in sub-sets and that is specifically aimed towards ensuring the privacy of sensitive transactions. Each channel within the network maintains a separate ledger that consist of two parts; the world state and the transaction state.[97] The Hyperledger network operates a very modular architecture which means every aspect of the network such as identity management, consensus and encryption can be selected from a ranging menu of options providing a comprehensive yet customisable network.[98] Basically, entities that wish to use the network can select specifics from the menu and customise them in a manner that suits the desired end use or objective.

(c) Quorum

The Quorum is a blockchain solution that was built on Ethereum (blockchain 2.0) and it seeks to instil the permissioned structure and privacy controls necessary for enterprise use, specifically financial enterprise use.[99] The privacy feature conceptualised for Quorum prevents all but the authorised parties to have access to information in respect of specific transactions through the smart contract protocol that provides for private data segmentation.[100] As a result, the solution maintains both public and private databases that are secured by smart contracts coded in a way that determines if information is private or public and then distributes it accordingly. This means, a node not party to a specific private contract cannot store

[96] Patel D & Ganne E, 'Blockchain and Distributed Ledger Technology in Trade: A reality check' (2019) 9.

[97] The world state ledger is similar to a database that contains the current state of the channel-specific ledger at any given time. On the other hand, the transaction state is an immutable record of all the transactions that have led to the current state of the world state. A transaction log can thus be used as a verifiable provenance trail for the ledger. (see Patel D & Ganne E (n 101) 19.

[98] Patel D & Ganne E (n 96) 19.

[99] Ibid., 20.

[100] Ibid.

the information even though the node is part of the blockchain network.[101] Loosely put, the in-built firewalls prevent parties who are not part of a specific private contract or transaction from having visual or access to the information that pertains to the transaction even though they are on the blockchain platform.

(d) Corda

The architecture of Corda employs a point-to-point data broadcast system which eliminates the notion of a single principal ledger opting instead for transactional data to be shared only with those entities on the network specifically involved in the transaction.[102] Corda employs what is known as a state system for higher levels of privacy. Basically, a state is an immutable object representing a fact known by one or more nodes at a specific point in time and transactions consume current states as inputs, apply the desired action and propose a potential new state.[103] The moment the data is verified, the potential new states automatically replace the current states and the current states become marked as historic. The process continues with new information being fed on to the platform. Corda also has the smart contract feature.

The system binds all data on chain contracts to traditionally recognised written legal agreements outlining the intended use of each contract by allowing for an object of the agreement to be included in the code.[104] Arguably, this helps circumvent, in the meantime, the grey area shrouding the legality and enforceability of smart contracts. Needless to say, there is need for a regulatory framework that specifically addresses the legality of smart contracts. In addition, Corda is a permissioned network with certified nodes only that are linked to registered and known entities thus providing an even extra layer of legal accountability.

While all the three types of blockchain infrastructure are exceptional in their own way with a number of benefits to entities, this study suggests that Hyperledger Fabric as best suitable for customs administration. This argument is based on the fact that it is a consortium permissioned platform which means it can be controlled by a number of different entities at once but with the same level of privacy as a private permissioned platform. As a consortium blockchain, it overcomes some of the challenges of private blockchains associated with having a single point of control. Consortium blockchains are less vulnerable to attacks or risks of attacks by third parties.

Furthermore, the architecture of the Hyperledger Fabric allows for customs administrations to customise the platform in a manner that enhances interoperability for seamless exchange of information. As indicated earlier, every aspect of the network including identity management and encryption of data can be customised to suit the objectives of the end user which allows customs administrations some degree of flexibility. In respect of privacy, the infrastructure keeps participants in sub-sets and participants who do not belong to the other sub-sets do not have visuals or access to data or information being exchanged. This

[101] Ibid.
[102] Ibid., 19.
[103] Ibid.
[104] Ibid., 20.

means that, stakeholders not part of a particular trade transaction cannot access information on that transaction. Only participants authorised in the sub-set can have access and visuals. In addition, information stored on to the platform by customs administrations that is considered sensitive cannot be accessed by all the other participants on the platform. That ensures a degree of privacy for sensitive transactions whilst maintaining full disclosure for customs control purposes.

3.3. Blockchain Features that can be Leveraged in Customs Administration

The WCO in its 2019 report identified the following as features of blockchain technology that can be leveraged by customs administrations:

- Blockchain operates on a distributed, rather than centralised platform with each participant having access to exactly the same ledger records subject to privacy considerations that govern each individual platform;
- The technology provides trust between and among unknown parties to transact and exchange information without an intermediary whilst ensuring data integrity at the same time, providing a full audit trail;
- Transactions are verified and approved by consensus among the participants in the network making fraud more difficult; and
- The full chronology of transactions that take place are tracked, thus allowing anyone with access including regulatory authorities to trace or review prior transactions.[105]

The Australian government affirmed the position by stating that blockchain technology is best suited in cases requiring at least three of the following factors:

- Data redundancy;
- Information transparency;
- Data immutability; and
- Consensus mechanism.[106]

Blockchain allows parties to a trade transaction to share real-time data that is open and accessible to everyone authorised to be on the platform. In practical terms, blockchain could be embedded into customs practices through a common platform which embraces trade-related commercial entities regularly engaged in the trading system such as banks, shipping lines, customs brokers and insurers.[107]

More so, blockchain has the potential to make visibility of data throughout the supply chain easier from end to end. The WCO argues that information on any transaction whether it be proof of purchase, invoices, clearance forms, bills of lading and insurance documents can be made part of a blockchain platform accessible to suppliers, transporters, buyers, regulators including customs and auditors.[108] This allows customs administration to have full access and 360-

[105] World Customs Organisation (n 63) 18.
[106] Department of Industries, Science, Energy and Resources, 'The National blockchain roadmap: Progressing towards a blockchain empowered future' A 2018 Blockchain Report by the Government of Australia https://www.industry.gov.au/blockchain (accessed 1 August 2022).
[107] Okazaki Y (n 64) 18.
[108] Ibid., citing Botton N (2018) 'Blockchain and Trade: Not a Fix for Brexit, but could revolutionise

visibility of all the information that is exchanged between and among parties to a transaction from the exporter to the importer.

In addition, the fact that information is open- ended and available for customs administrations in real-time can potentially help with customs declarations. The creation of customs declaration documents is a cumbersome process and the most common impediment relate to collecting and verifying the information from different stakeholders.[109] Blockchain-based solutions can help expediently collect information available the moment it is uploaded. Also, once entered, the information is immutable meaning it cannot be altered or changed which builds confidence on the trustworthiness of data.

Currently, customs officials face challenges with receiving electronic information and sharing it with other agencies. This is due to low data quality, delays in the submission of the requested data, potential inadvertent or deliberate mistakes in data due to it changing through multiple hands and insufficient capacity for data verification. The WCO argues that blockchain can overcome the challenges in that it allows for instantaneous sharing of data through permissioned networks in a trusted and secure manner.[110] By using a common distributed technical platform, customs administrations could leverage the power of blockchain to share information and resources particularly in a Single Window environment and for cross-border data exchange purposes.[111]

Generally, users need confidence about where the data on the network comes from (provenance), that the data is accurate, without any accidental or deliberate errors (integrity) and that appropriate systems are in place to manage how the data is entered.[112] Blockchain platforms guarantee security, provenance, integrity and better governance of data that is entered on to the platform which would work best in customs administration where trust is required. Blockchain platforms also allow for classification of data based on how trustworthy the source for the data is. Data from highly reliable sources such as banks and other customs administrations will be classified as having high level of trust and data from less reliable sources can then be classified as having low levels of trust.[113] This helps customs administrations put in place additional measures to authenticate data that would have been submitted by less trustworthy sources.

3.4. Concerns

There are concerns that have been raised critiquing blockchain technology and these relate to data protection, legal challenges and the decentralised nature of the technology itself. These shall be addressed in detail below.

Global Value Chains (if Governments Let it) European Centre for International Political Economy.
[109] World Customs Organisation (n 63) 21.
[110] World Customs Organisation (n 63) 22.
[111] Okazaki Y (n 64) 17.
[112] Department of Industries, Science, Energy and Resources, Government of Australia (n 106) 16.
[113] Ibid.

3.4.1. Personal data privacy and protection

One of the main concerns that have been raised in relation to the use of blockchain technology relates to the privacy and protection of personal data. This emanates from the fact that data entered on to a blockchain network cannot be erased and this seems to contradict the legal steps that are currently being taken in a number of jurisdictions towards personal data protection. For instance, the European Union's General Data Protection Regulation (GDPR) provides for the right to erasure or the right to be forgotten. In terms of Article 17 of the GDPR a data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.[114]

The immutable nature of blockchains, and arguably the core of their value disposition prevents data from being deleted which poses a challenge for current and potential users.[115] Organisations are always trying to come up with a work-around to this issue. The *Commission Nationale de l'Informatique et des Libertés* (CNIL), an independent French administrative regulatory body whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data, proposed some workaround to this inconsistency.[116] The Commission proposed that that the processing and storing of data should be done off-chain, and that the data recorded on the blockchain itself should only be a commitment, a hash generated by a keyed-hash function or a cipher text obtained through "state of the art" algorithms and keys.[117] This makes the data practically inaccessible although it can still be verifiable.

However, it is important to note that it is technically impossible to grant the request for rectification or for erasure made by a data subject when clear text or hashed data has been recorded on a blockchain network.[118] Therefore, there is need for further work in trying to figure out how the networks can be used in a manner that balances with the needs of a data subject to have their personal data protected. Maybe, solace can come from the fact that the data is only visible to authorised parties and the technology itself prevents the sharing of same with unauthorised parties.

(e) Legal challenges

The use of blockchain technology presents quite a number of legal concerns. The network uses electronic signatures, electronic documents and in some instances smart contract. However, these technological tools are not yet legally recognised in most jurisdictions. Although the United Nations Commission of International Trade Law (UNCITRAL) adopted a model law on electronic signatures in 2001, the formal recognition of electronic signatures on negotiable

[114] General Data Protection Regulation (EU) 2016/679.
[115] Patel D & Ganne E (n 96) 49.
[116] Ibid; see also, Bundesministerium der Finanzen 'Blockchain strategy for the Federal Government: We set out the course for the Token Economy' (2020) 12 The Government of Germany Blockchain Strategy.
[117] Patel D & Ganne E (n 96) 50.
[118] Ibid.

documents is yet to be solidified in a number of jurisdictions.[119] Hopefully, the negotiators of the AfCFTA will consider including such issues during phase three negotiations of the Protocol on Digital Trade.

Furthermore, the development of smart contracts that make it easier to execute transactions on the network without the intervention of third parties has challenged the application of the conventional law of contract. The actual function of a smart contract is inherently different from that of a conventional contract mainly because the former is a self-executing transaction that is written in computer code and performed in an automated way.[120] For instance, the code could be written with an instruction to automatically transfer money from one account to the other the moment a bill of lading is fed on to the network. This is fundamentally different from how conventional contracts work and the challenge becomes, what laws should apply to adjudicate dispute that arise from smart contracts? This remains a grey area that needs to be addressed.

Also, the way distributed ledgers generally are conceptualised, there is no consensus algorithm or any computer algorithm for that matter that is capable of determining whether a certain transaction has occurred as a result of a legally enforceable contract or not.[121] That also poses a legal challenge for the participants. Therefore, there is need for a clear regulatory framework that regulates the use of digital technological tools in the business environment. The current frameworks are becoming redundant, thus, there is need to update them to suit the technological changes currently happening.

(f) The decentralised nature of blockchain

Blockchain technology is decentralised in nature. Critics have argued that because it lacks a centralised oversight function and has no effective trouble-shooter which should work in the event of contingency, it compromises the resilience of the entire system.[122] What this means is that in the event of an attack or threat, each participant could suffer directly from the external shock. However, it is important to note that in reality, the decentralised nature of the technology actually makes it less susceptible to attacks especially external attacks. The network system lacks what is known as a Single Point of Failure (SPF).[123] An SPF when attacked takes down the entire system and automatically prevents it from working.

The decentralised nature of the technology is actually a huge incentive for blockchain users. A network comprising of a number of participants cannot stop working unless at least 51 percent of the users has been captured at once. The 51 percent attack basically entails that an attacker o can interfere with the data recording onto a network if they manage to have at least 51 percent of control of the computing power on the network at once. In other words, the attackers need to

[119] Patel D & Ganne E (n 96) 48.
[120] Sanitt A & Green S 'Smart Contracts' in Davies P and Raczynska M (eds) '*The Contents of Commercial Contracts: Terms Affecting Freedoms'* (2019) 2.
[121] Patel D & Ganne E (n 96) 48.
[122] Okazaki Y (n 69) 9.
[123] A Single Point of Failure is the part of the system that, if it fails, it takes down the entire system too. If hit during an attack, it collapses the whole system and prevent the whole system from working.

be in control of at least 51 percent of the computers that are being used on the platform which is highly unusual especially in international trade supply chain. There have been debates on whether the 51 percent attack rule means that smaller blockchain networks could be vulnerable to attacks, but the developers and cryptography community have not reached a verdict yet.[124] However, the fact remains that the bigger the network, the more tamper resistant it will be.[125]

3.5. Case Studies on the Use of Blockchain Technology

There are quite a number blockchain based solutions that have been implemented in the supply chain system. For the purposes of this study, case studies will be limited to those implemented in customs administration so as to justify why African countries should consider blockchain-based solutions for trade facilitation.

3.5.1. Egypt's CargoX

Egypt launched the CargoX as the official document transfer platform for the country's Advance Cargo Information (ACI) system in May 2021.[126] The ACI is a WCO protocol to provide shipping lines, port operators and governments with real-time information on shipments of incoming goods.[127] The ACI declarations are currently being submitted though National Single Window for Foreign Trade Facilitation (NAFEZA) platform which was built on the Misr Technology Systems (MTS).[128] NAFEZA is a Single Window concept that was implemented to facilitate electronic trade and standardise information and documentation through a unified regulatory environment.[129]

CargoX was built to enhance NAFEZA's efficiency. The platform is powered by the Ethereum technology and was built to integrate and coordinate procedures and information exchange between all parties involved in Egypt's foreign trade system.[130] Using CargoX for ACI allows customs authorities to stop relying on declarations from importers as each document can easily be traced back to its origin, directly to the issuer.[131]

---

[124] Okazaki Y (n 64) 9.
[125] Ibid.
[126] Research Alert 'Egypt: Authorities to use blockchain-powered Advance Cargo Information System' (*Research Alert, Middle East and Africa-Trade Investment* 3 May 2021) https://research.hktdc.com/en/article/NzM3MjMyMDk5#:~:text=The%20Egyptian%20authorities%20confirmed%20in,Cargo%20Information%20(ACI)%20System.&text=The%20government%20of%20Egypt%20is,ACI%20system%20using%20blockchain%20technology. (accessed 5 August 2022).
[127] Ibid.
[128] Ibid.
[129] Shalaby MJ 'NAFEZA: Building Digital Trust- The truth about exporting to Egypt using their new one-window system,' (*Linkedin* 30 March 2021) https://www.linkedin.com/pulse/truth-exporting-egypt-using-new-one-window-system-shalaby/ (accessed 5 August 20222).
[130] Transaport and Logistics 'CargoX authorised as Egypt's blockchain document transfer gateway' (*Transport and Logistics Middle East,* 21 April 2021) https://www.transportandlogisticsme.com/smart-technology-innovation/cargox-authorized-as-egypts-blockchain-document-transfer-gateway (accessed 5 August).
[131] Shalaby MJ (n 129).

As from 1 July 2021, importers became obliged to record key data about their imports into the system, for assessment by customs and other relevant authorities, if it is acceptable a unique identification number is issued within 48 hours.[132] The shipper then has to provide a list of the cargo that is automatically verified against what would have been specified and approved.[133] The said data posted on to the platform will be accessible by stakeholders in the supply chain including the importer, exporter and shipping agents in real time. The government enacted the Egyptian Customs Law No.207 of 2020 which provides for the use of ACI declarations. The blockchain-based solution is thus an infrastructure that has been set to support the application of the Act. Egypt is one of the first countries in the world to implement a digital ACI using blockchain technology and the system is currently operational.

The Egyptian initiative seems to answer the longstanding question regarding the interoperability of blockchain technology. Interoperability has been raised as a concern particularly in relation to the technology's ability to interoperate with other technologies. The architecture of CargoX made it possible for the network to interoperate with NAFEZA which a completely different technology. This addresses one of the pain points for Single Windows which is their inability to interoperate. As stated earlier, lack of interoperability is one the main reasons why the current single window architecture makes it difficult for customs administrations to seamlessly share trade data in a timely manner due to the isolated nature of the data gathered.[134]

3.5.2. TradeLens

International Business Machines Corporation (IBM) and Maersk developed a trade platform called TradeLens, powered by the Hyperledger Fabric to digitalise the entire supply chain ecosystem. The platform is designed to facilitate sharing of end-to-end supply chain information and documentation across the large number of divers and independent parties that are involved in a typical trade transaction.[135] As of November 2019 when Trade Finance Global conducted a study on TradeLens, the ecosystem had over 180 members; two thirds of all container shipping lines globally, over 80 terminals and posts, 17 customs authorities, a dozen of inland providers, banking services, global and regional freight forwarders live on the platform.[136] In addition, more than 2 million events and over 15 000 documents are transmitted through the platform daily.[137]

3.5.3. Peruvian CADENA tool

CADENA was developed by Microsoft with the sponsorship of the Inter-American Development Bank to be a tool for digital mutual recognition of

[132] Research Alert (n 126).
[133] Ibid.
[134] World Economic Forum (n 1) 13.
[135] Patel D & Ganne E (n 96) 41.
[136] Ibid.
[137] Ibid.

Authorised Economic Operator (AEO) certificates.[138] The concept of AEOs provides for traders who voluntarily meet a range of criteria to work in close cooperation with customs authorities to ensure the common objective of supply chain security.[139] CADENA enables users to share a single view of the status of an AEO certificate in real-time which helps customs administrations process the certificates faster.[140] The developers of the solution envisioned a situation where CADENA is integrated with the IT systems of each customs administration to ensure that the benefits can be accessible in real-time.[141] In addition, the network is expected to solve the interoperability challenges that traditional ICT tools especially Single Windows are facing.

CONCLUSION

Single Windows maintained in Africa have successfully managed to reduce document processing time thus saving costs for traders. However, the main challenge that these Single Windows are facing currently is caused by the fact that they have not yet been fully implemented. As a result, they cannot interoperate and, in some instances, traders are still expected to submit trade documents manually which undermines the credibility of the information submitted.

The AfCFTA which was established to boost intra-African trade is going to be a success if African countries put in place measures to support the faster clearance of goods at border posts. Although the legal framework supports introducing and maintaining Single Windows, the current architecture of Single Windows is becoming redundant. Governments should consider leveraging the digital technologies that are coming up to try and resolve some of these challenges.

Blockchain technology can be the solution that Africa needs to revolutionise the Single Window architecture. The technology allows for faster processing time of documents as all entities involved in the supply chain can be part of the same network with real-time visibility of information. Also, smart contracts can assist in the faster settlement of invoices without the involvement of third parties. However, the successful implementation will only depend on the availability of resources and political will in Africa.

[138] The AEO concept is based on the customs-to-business partnership introduced by the World Customs Organisation (see European Commission 'Authorised Economic Operator (AEO)' https://ec.europa.eu/taxation_customs/authorised-economic-operator-aeo_en (accessed 2 August 2022).

[139] European Commission 'Authorised Economic Operator (AEO) https://ec.europa.eu/taxation_customs/authorised-economic-operator-aeo_en (accessed 2 August 2022).

[140] World Customs Organisation (2019b) 19.

[141] World Customs Organisation (2019b) 19.

LEGAL ISSUES ON ADMISSIBILITY OF ELECTRONIC SIGNATURES UNDER THE ELECTRONIC SIGNATURES ACT IN UGANDA'S CIVIL PROCEEDINGS

Paul Mukiibi*

ABSTRACT

The Electronic Signatures Act (ESA), 2011 has been in force for more than one decade now. It is an Act to make provision for and to regulate the use of electronic signatures and to provide for other related matter. There are concerns, however, whether documents signed electronically under this Act can be admissible in evidence. Specific attention has been put on affidavits and statutory declarations which require physical presence of a deponent or declarant before a commissioner for oaths, notary public or justice of peace. Accordingly, this article examines the challenges associated with e-signatures in civil proceedings. The article concludes that e-signatures have been embraced globally and are applied with principles of non-discrimination, technological neutrality and functional equivalence. Despite this, e-signatures are faced with challenges of parallel existing laws requiring physical presence and writing of a signature in the presence of an authorised officer. This happens during notarising, commissioning, attesting and sealing of such documents. Other challenges relate to absence of adequate public key infrastructure to manage the system, electronic print against handwritten print and the nature of an electronic signature under the ESA. The article recommends harmonizing laws governing admissibility of evidence in civil proceedings with ESA, technological infrastructure improvement, training efficient and reliable human resource infrastructure, use of password and hybrid methods to enhance security of the signature, licence more public key infrastructure and certification services providers, use of biometrics to safeguard the system, video witnessing of signatures, amending legislation that is incompatible with modern technology and training and sensitization facilities of all the stakeholders.

* MITPL (UMU); MBA (UMI); LLM (Mak); PG.Dip LP (LDC); LLB (Mak). Head, Department of Law Reporting, Research and Law Reform LDC; Lecturer LDC; and Part-Time Lecturer, Kyambogo University. Advocate; Commissioner for Oaths; and Notary Public. E-mail: pmukiibi@ldc.ac.ug

INTRODUCTION

In 2011, Parliament of Uganda enacted the Electronic Signatures Act (ESA).[1] This Act was assented by the President of the Republic of Uganda on 17 February 2011[2] and came into force on 18 March 2011.[3] The ESA among others was enacted to make provision for and to regulate the use of electronic signatures and to provide for other related matters.[4] Prior to this Act, signatures in any legal proceedings and transactions were only deemed authentic if they appeared in manual and physical form of a person or persons appending such signatures. Simply put, electronic signatures were not admissible under the law as they had no enabling law to enforce them. Reliance on admissibility of evidence was majorly governed by the Evidence Act of Uganda which provided no room for electronic signatures.[5]

With the coming into force of ESA, it was hoped that appending signatures on legal documents would become more easier especially on categories of persons who are very far, or outside jurisdiction and their evidence is very critical in specific legal proceedings. Indeed, the legislator intended to avoid wastage of time and costs to have a person physically append a signature on a particular document and manually transport the document to the destination it is needed to be relied upon in evidence in legal proceedings. Consequently, legal documents like tenancy agreements, mortgages, land sale and purchase agreements, powers of attorney, witness statements, among others can pass the test of validity if they conform to the provisions of the ESA.[6]

Although the ESA came into force in 2011 and prior to the declaration of Covid-19 as a global pandemic by the World Health Organisation (WHO), on 18th March 2020, the Government of Uganda (GOU), through the Office of the President, announced a series of public health measures to prevent the spread of Covid-19 across the country.[7] This ushered in the first lockdown in the country since the declaration of Covid-19, a global pandemic by the WHO. The same announcement was repeated on 18th June 2021 which ushered in a second lockdown.[8] Of concern

[1] Act No. 7 of 2011.
[2] See Date of Assent in the Act itself.
[3] The Act commenced on 18 March 2011. See The Uganda Gazette No. 19 Volume CIV dated 18 March 2011. Printed by UPPC, Entebbe, by Order of the Government.
[4] See the Long title to ESA.
[5] The Evidence Act Cap. 6, Laws of Uganda came into force on the 10th day of December 1963. Electronic evidence in Uganda then was unheard of.
[6] See Sec. 4 (3) of the ESA on reliability of an electronic signature.
[7] *See* for e.g., COVID-19 Guidelines for mass gatherings, available at <www.COVID-19-GUIDELINES-FOR-MASS-GATHERINGS.pdf> (accessed 26 November 2021); Africa News, Uganda imposes another lockdown: What are the restrictions? 7 June 2021, available at <https://www.africanews.com/2021/06/07/uganda-imposes-another-lockdown-what-are-the-restrictions> (accessed 26 November 2021).
[8] *Ibid.*

to this article is that electronic signatures applied so much on legal documents as they were considered among the protective measures to avoid the spread of the pandemic, despite the fact that very few Ugandans can use this kind of technology. This among other concerns justifies the relevance of the legislation which perhaps the legislator had not thought about in 2011.

At the coming into force of ESA, there were other laws governing evidence in Uganda's civil procedure, specifically, the Evidence Act;[9] the Oaths Act, Cap 19;[10] the Statutory Declarations Act, Cap 22;[11] and the Civil Procedure Rules, SI.71-1.[12] These legislations are still in force notwithstanding the coming into force of the ESA. Some of these laws for example require a deponent or declarant to append his or her signature on an affidavit or declaration as proof that he or she made such an affidavit or declaration.[13] The requirement goes further to demand such a deponent or declarant to do so before a commissioner for oaths or a person authorised under the law to administer oaths in Uganda.[14] This in itself may require physical presence of the deponent or declarant before such a commissioner for oaths and the presumption of the law is that such a person appends his or her signature physically before the commissioner for oaths or the officer authorised to administer oaths under the law.[15] This brings in context concerns as to whether the framers of the ESA had in mind that affidavits and statutory declarations are legal documents and whether the same can be subjected to the provisions of the ESA.

In civil and common law countries, the enforceability of many types of contracts is subject to certain formalities. The most common formality is the requirement of a contract reduced in writing signed by the parties to it. In Uganda as in other commonwealth jurisdictions written contracts would necessitate signification of agreement. Furthermore, the witnessing of that signification is also desired. Such signification is generally manufactured in terms of personified marks such as signatures and seals. Further proof by witnesses is desired.

The above concerns give rise to legal issues as to whether an affidavit or declaration can be made electronically or subjected to electronic signature under the ESA when the law requires the deponent or declarant to physically appear before the officer administering the oath before signing the said affidavit. Against this backdrop, this article critically examines the legal issues surrounding admissibility of electronic signatures under the ESA in Uganda's civil proceedings.

---

[9] Cap. 6, Laws of Uganda

[10] Sec. 5 (1) of the Act gives the way an oath can be taken. The third schedule gives a form of a jurat that is made by the officer administering the oath and must state that the deponent or declarant appeared before him or her.

[11] Sec. 5 (1) of the Act requires a judge, the registrar, a magistrate, or a justice of the peace, a notary public and any commissioner for oaths to take and receive the statutory declaration of any person voluntarily making it before him or her and shall certify it under his or her signature. See also Sec. 6 (1) & (2) regarding taking out statutory declarations outside Uganda.

[12] S.I. 71-1 (as amended by S.I. NO. 33/2019).

[13] *Supra at 12*.

[14] *Ibid.*

[15] *Ibid.*

It analyses the inception of e-signatures in Uganda, challenges associated with use of e-signatures in Uganda's civil proceedings and measures to improve the use of e-signatures in Uganda's civil proceedings.

The article is presented under the following themes: (a) electronic evidence, electronic signatures and digital signatures; (b) admissibility of electronic signatures; (c) effectiveness of electronic signatures; (d) international, regional and domestic instruments on electronic signatures; (e) a review of court decisions on the authenticity of electronic signatures; (f) challenges associated with electronic signatures; and (g) recommendations.

2. ELECTRONIC EVIDENCE, ELECTRONIC SIGNATURES AND DIGITAL SIGNATURES

2.1. Electronic Evidence

Different jurisdictions have attempted to define electronic evidence, however, there is no specific definition per se. Some precepts defining the term, however, exist. The Finnish legal Proceedings Code refers to it as "deeds that support action,"[16] meaning both the digital support and the paper support. A more direct reference exists in the Police & Criminal Evidence Code of the United Kingdom: "evidence is all information contained in a computer."[17] This equally does not give a precise definition of the term.

George and Stephen Mason define electronic evidence as all information with probative value that is included in an electronic media or is transmitted by media.[18] They further give an expansive definition as data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication.[19]

Electronic evidence is derived from electronic devices such as computers and their peripheral apparatus, computer networks, mobile telephones, digital cameras and other portable equipment (including data storage devices), as well as from the internet. The information it contains does not possess an independent physical form.[20]

However, in many ways, electronic evidence is no different from traditional evidence in that the party introducing it into legal proceedings must be able to demonstrate that it reflects the same set of circumstances and factual information as

[16] Legal Proceedings code of Finland. Chapter 17, Section 11b.
[17] Police and Criminal Evidence Act, PACE, United Kingdom.
[18] Electronic Evidence, George, Madson University of London Press, Institute of Advanced Legal Studies, 2017. Available at https://www.jstor.org/stable/j.ctv512x65 accessed on 09 June 2022.
[19] *Ibid.*
[20] Electronic Evidence Guide. A Basic Guide for Police Officers, Prosecutors and Judges. European Union, 2014. p. 11.

it did at the time of the offence.[21]

In other words, they must be able to show that no changes, deletions, additions or other alterations have (or might have) taken place. The intangible nature of any data and information stored in electronic form makes it much easier to manipulate and more prone to alteration than traditional forms of evidence. This has created special challenges for the justice system which requires that such data be handled in a special way to ensure the integrity of the evidence it offers.[22]

Given its special characteristics, electronic evidence could be defined as: any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings.[23]

In Uganda, the term is neither defined under the ESA nor the Electronic Transactions Act.[24] Courts of record have however, attempted to define the term electronic evidence. *Justice Margaret Mutonyi* in the case of *Amongin Jane Francis Okili Vs Lucy Akello and The Electoral Commission*[25] has defined electronic evidence as any probative information stored or transmitted in digital form that a party at a trial or proceeding may use. It is used to prove a particular proposition or to persuade court of the truth of an allegation.

2.2. Electronic Signatures

In the network environment, e-government and e-commerce are dependent on electronic documents and signatures as the foundation of electronic communications and transactions. In order to encourage the development of digital economic activity, the norm for legal electronic documents and signatures according to the Law of E-Signature is required. Legitimizing e-signature to set up a safe and authentic environment for electronic transactions that incorporate e-commerce applications has become a global issue.[26] Nowadays, the technology of e-signature can be applied to purchase on the internet, distance education, web entertainments, and internet finance such as the electronic trading of stocks and bonds.

An e-signature consists of e-signature image and digital signature. E-signature is generally associated with a number of technologies, allows a person (or machine) to electronically mark a document,[27] and can enable innovative document management processes.[28] In other words, e-signature provides electronic

[21] *Ibid.*
[22] *Ibid.*
[23] *Ibid.*
[24] Act No. 8 of 2011.
[25] HCT-02-CV-0001-2014. Available at https://ulii.org/ug/judgment/election-petitions/2015/1 accessed on 09 June 2022.
[26] MOEA Electronic Signatures Act, Ministry of Economic Affairs, R.O.C. 2002. http://www.esign.org.tw/English.asp Accessed on 09 June 2022.
[27] Nunnally J.C. 2nd ed. McGraw-Hill; New York: 1978. Psychometric Theory. [Google Scholar]
[28] Nunno R.M. Electronic signatures: technology developments and legislative issues. *Government Information Quarterly.* 2000;17(4):395–401. [Google Scholar]

authentication and a process to verify the identity of users with a stand-alone mainframe, network, or internet-based system to control access or authorize transactions.[29]

There are many forms of e-signature. Benjamin Wright, a noted e-commerce attorney and co-author of The Law of Electronic Commerce, concluded that "How, where, and when e-signatures are used requires the same care and common sense that one would apply to the use of pen and ink signatures".[30] In many states and industry sectors of the US, e-signatures attached to electronic records (documents created, stored, generated, received, or communicated by electronic means) are legally recognized in the same manner as handwritten signatures on paper.[31]

The term "electronic signature" is defined under the ESA to mean data in electronic form affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message; and includes an advance electronic signature and the secure signature.[32]

The ESA further defines "electronic signature product" to mean configured hardware or software or relevant components of it, which are intended to be used by a certification service provider for the provision of electronic signature services or are intended to be used for the creation or verification of electronic signatures.[33]

On the other hand, "advanced electronic signature" is defined both under the ESA[34] and Electronic Transactions Act[35] to mean an electronic signature, which is: (a) uniquely linked to the signatory; (b) reliably capable of identifying the signatory; (c) created using secure signature creation device that the signatory can maintain under his sole control; and (d) linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and signature are detectable.

2.3. Digital Signatures

The ESA defines a "digital signature" to mean a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (a) whether the transformation was created using the private key that corresponds to the signer's public key; and (b) whether the message has been altered since the transformation

[29] Poon P., Wagner C. Critical success factors revisited: success and failure cases of information systems for senior executives. *Decision Support Systems.* 2001; 30:393–418. [Google Scholar]

[30] Premkumar G., Ramamurthy K. The role of interorganizational and organizational factors on the decision mode for adoption of interorganizational systems. *Decision Sciences.* 1995;26(3):303–336. [Google Scholar]

[31] Premkumar G., Roberts M. Adoption of new information technologies in rural small business. *Omega.* 1999;27(4):467–484. [Google Scholar]

[32] See Sec. 2 of the ESA.

[33] *Ibid.*

[34] *Ibid.*

[35] See Sec. 2 of the Act.

was made.[36]

Digital signatures involve the use of the hash function. A digital signature permits signing a message in order to enable detection of changes to the message contents, to ensure that the message was legitimately sent by the expected party, and to prevent the sender from denying that he or she sent the message, known as nonrepudiation. To digitally sign a message, the sender would generate a hash of the message, and then use his private key to encrypt the hash, thus generating a digital signature. The sender would then send the digital signature along with the message, usually by appending it to the message itself.[37]

When the message arrives at the receiving end, the receiver would use the sender's public key to decrypt the digital signature, thus restoring the original hash of the message. The receiver can then verify the integrity of the message by hashing the message again and comparing the two hashes. Although this may sound like a considerable amount of work to verify the integrity of the message, it is often done by a software application of some kind and the process typically is largely invisible to the end user. A digital signature is considered legally binding and if it is lost or stolen must be revoked.[38]

Digital signatures are very different from the handwritten signatures used on paper. Because data on a computer can be easily copied, an image of a person's written signature could be cut and pasted into a new document, making signature forgery a simple task. A different type of signature had to be designed for the digital realm.[39]

Digital signatures can provide data integrity, authentication, and support for nonrepudiation. After a message has been signed, it cannot be modified without being detected. A valid digital signature can only be created by the original signer (i.e., cannot be forged) and thus can prove who signed the message. While signature creation relies on private information, signature verification must be possible with public information. The signer cannot later deny signing the message.[40]

In today's digital world, the average person doesn't think twice about using electronic signatures, however, the position for practitioners like attorneys is different. Attorneys should be more cautious with electronic signatures. Over the past 20 years, electronic signature use has been on the rise globally. Due to their convenience, they are now used daily in myriad contracts and agreements. Practitioners, however, should consider the applicable statutes and practical downsides to using electronic signatures. Electronic signatures present unique issues in litigation. For example, an electronic signer can more easily deny that he

[36] Sec. 2 of the ESA.

[37] Jason Andress, in The Basics of Information Security (Second Edition), 2014 https://www.sciencedirect.com/topics/computer-science/digital-signature. Accessed on 09 June 2022

[38] *Ibid.*

[39] Jeff Gilchrist, in:
Encyclopedia of Information Systems, 2003, https://www.sciencedirect.com/topics/computer-science/digital-signature. Accessed on 9 June 2022

[40] *Ibid.*

actually signed the document. And it may be difficult to determine how to lay proper foundation for an electronic signature.

In the next section, the article examines the admissibility of electronic signatures and examines the burden of proof in proving the validity of such a signature.

3. ADMISSIBILITY OF ELECTRONIC SIGNATURES

Consider this common question: how will an electronic signature hold up if challenged in court? After all, electronic signatures are becoming a vital business tool in today's remote environment and people want to know if they end up in litigation that the authenticity of an e-signature can be proved like a traditional wet signature. Authenticity is easier to prove, in fact, thanks to built-in digital audit trails. In disputes over agreements, courts are sometimes charged with establishing whether a signature is valid and attributing it to the signer, based on an evidentiary burden of proof. A digital audit trail does that brilliantly and in a way that other methods can't touch, because the data captured around an electronic signature provides more concrete evidence around the authenticity of someone's signature, and thereby their obligations under a contract, making it easier to meet the burden of proof.[41]

Practitioners thus need to check local rules regarding the use of electronic signatures to avoid potential sanction. In December 2016, a bankruptcy judge for the Eastern District of California imposed sanctions on a bankruptcy lawyer for permitting a debtor client to use DocuSign to sign documents requiring an original signature. In *Re Mayfield*,[42] the bankruptcy attorney submitted various documents which the debtor had signed using DocuSign. The United States Trustee argued that DocuSign did not constitute an original ("wet") signature as required under the applicable bankruptcy and local rules. The court noted its concerns that an electronic signature could be more easily forged, or placed by someone other than the debtor, leading to potential disputes over the validity of critical case documents.[43] The essential point is that an individual's handwritten signature is less easily forged than any form of software-generated electronic signature, and the presence of forgery is more easily detected and proven.

Typically for wet signatures, validity and attribution are established by comparing copies of signatures and presenting testimony from handwriting experts or witnesses who were present at the signing. Not only is this expensive and time

[41] Tyler Newby, Partner at Fenwick & West LLP does a fantastic job outlining just how valuable audit trails are in authenticating e-signatures in court in his article, "Using E-Signatures in Court—The Value of an Audit Trail." Available at https://www.fenwick.com/publications/Pages/Using-E-Signatures-in-Court-The-Value-of-an-Audit-Trail.aspx (accessed on 5 August 2022).

[42] [2016] WL 3958982, No. 16-22134-D-7.

[43] Available at https://www.govinfo.gov/content/pkg/USCOURTS-caeb-2_16-bk-22134/pdf/USCOURTS-caeb-2_16-bk-22134-0.pdf (accessed on 5 August 2022).

consuming but also less reliable due to the human element. By removing the chance for human error and automating the entire data capturing process, audit trails make it easier to establish authenticity and address disputes over signatures in courts of law.

In his article, Newby outlines a variety of cases where audit trails were effective in establishing a signatory because of information they contain. Data establishing IP addresses, date, time and location for when a contract was received, viewed and signed has proven particularly relevant to establishing signature authenticity.[44] One state case that Tyler cited, *IO Moonwalkers, Inc. v. Bank of America*,[45] went as far as to say that the DocuSign system established an electronic trail of information (send, receipt, signature, review) that wasn't available before the digital age and is a more credible method of establishing evidence than a sworn statement of whether an agreement was sent via mail.

All audit trails are not created equal, so how the audit trail is set up is crucial. If done right, there's an amazing amount of case law to support their admissibility in court. The DocuSign eSignature audit trail includes all the components mentioned in the case law and follows a secure and documented process necessary for court admissibility. This includes inter alia: a complete, automated history of every viewing, printing, sending, signing or declining activity, including key event timestamps; Identifying data, such as the signer's IP address or officially affiliated email address; Geolocation of signers, if they agree to share that information; A tamper-evident seal that validates documents haven't been altered outside of each signing event; A court-admissible certificate of completion available to all participants in the transaction; Multiple levels of authentication based on email, access code, SMS, phone, geo-location, among others.[46]

DocuSign also takes a security-first approach to e-signatures to ensure all audit trails, certificates of completion and customer documents that flow through the DocuSign Agreement Cloud stay safe, secure and unaltered before, during and after signing.[47]

In the next section, the study examines the legal purpose of a signature and what makes it effective in civil transactions and proceedings.

4. EFFECTIVENESS OF ELECTRONIC SIGNATURES

A manuscript signature is accepted without question as legally effective in all jurisdictions, assuming it has not been procured by fraud, and it is rarely asked

[44] *Ibid*

[45] [2018] 814 S.E.2d 583.
Available at https://www.courtlistener.com/opinion/4483402/io-moonwalkers-inc-v-banc-of-am-merch-servs/ (accessed on 5 August 2022).

[46] Available at https://www.docusign.com/trust/security/product-security (accessed on 5 August 2022).

[47] *Ibid*

what effects such a signature is required by law to achieve. However, in those cases where the validity of alternatives has been considered, other methods of signing a document, such as signature by means of a printed or rubber stamp facsimile, have been assessed for validity. The most common approach is to define the functions that a signature must perform, and then to treat signature methods that affect those functions as valid signatures. The primary function of a physical signature is to provide evidence of three matters: the identity of the signatory; that the signatory intended the signature to be his signature and that the signatory approves of and adopts the contents of the document.

Manuscript signatures meet these functional requirements in a number of ways. Identity is established by comparing the signature on the document with other signatures that can be proved, by extrinsic evidence, to have been written by the signatory. The assumption is that manuscript signatures are unique, and that, therefore, such a comparison is all that is necessary to provide evidence of identity. In practice, manuscript signatures are usually acknowledged by the signatory once they are shown to him, and extrinsic evidence is only required where it is alleged that the signature has been forged.

Also, intention to sign is normally presumed because the act of affixing a manuscript signature to a document is universally recognized as signing. Intention to sign is normally only disputed where the affixing of the signature has been procured by fraud, and in those cases the signatory bears the burden of displacing the presumption that he intended to sign. Intention to adopt the contents of the document is similarly presumed because it is general knowledge that affixing a manuscript signature to a document has that effect. In both cases, the burden of displacing the presumption is on the signatory.[48] The following explanation has been offered by the Sri Lankan Ministry of Justice:

> In the context of Internet communications, the thing to be signed, an electronic document, exists more as a matter of metaphysics than as a physical object. For this reason, it is very difficult for an electronic signature method to meet any physical requirement of form.[49] For example, some of the English cases and statutes on physical world signatures appear to state that a signature must take the form of a mark on a document.
>
> An electronic signature, by itself, cannot provide sufficient evidence of the signatory's identity. To explore this matter further, evidence is required that links the signature key or other signature device to the signatory himself. But the

[48] Ministry of Justice, Sri Lanka, 'Electronic Signatures – Perspectives and Problems', available at:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiomYuJ15qAAxXL6aQKHf2cDZsQFnoECAgQAQ&url=https%3A%2F%2Fwww.lawnet.gov.lk%2Felectronic-signatures-perspectives-and-problems%2F&usg=AOvVaw2c89cR8a0VHtTtrB-dxOSm&opi=89978449

[49] See, e.g., *Saunders v. Anglia Bldg. Society* [1971] AC 1004.

> recipient wishes to be able to rely on the signature without needing to collect evidence for use in the unlikely event that the signature is disputed. For this reason, most electronic signatures used for e-commerce communications are likely to be accompanied by an ID Certificate issued by a Certification Authority. The Certification Authority takes traditional evidence of identity, for example, by examining passports, and, in the case of public key encryption digital signatures, checks that signatures effected with the signatory's secret key are verifiable using the public key. Once the Certification Authority is satisfied as to the signatory's identity, it issues an ID Certificate, which includes, inter alia, a certification of the signatory's identity and of his public key. This certificate may be used by the recipient to prove the signatory's identity.
>
> It is useful to look at how analog "wet ink" signatures are authenticated in court when, for example, a party attempts to show that the scribble on a signature block is the signature of another party. If contested, parties typically have used comparisons between known signatures and the questioned signature with corroborating witness testimony that a separate individual saw the signing of the document or the testimony of handwriting experts confirming the similarity of the signatures. All the proponent needs to produce is "sufficient" evidence that the signature is that of the other party; questions as to the strength of that evidence will go to the weight the fact finder gives the evidence in court.
>
> E-signatures backed by an audit trail help clear this low authenticity bar even more easily. Audit trails are digital records maintained by the e-signature service that, among other things, identify when a document was sent, opened and signed, as well as the names, email addresses and unique signing identifiers of the signatories. They also may include records like IP addresses or machine IDs to further trace when and where a document was opened and signed.[50]

In the next section, this article examines the international, regional and domestic instruments governing admissibility of e-signatures in different jurisdictions.

5. INTERNATIONAL, REGIONAL AND DOMESTIC INSTRUMENTS ON E-SIGNATURES

International trade has evolved over the years with electronic commerce taking centre stage in how international business is conducted. The use of electronic signatures has streamlined international trade by reducing the time involved to exchange physical documents signed by parties to a global business transaction. Clearly, the legal validity of electronic signatures is of international importance since no progress can be made in developing the legal institutions needed for conducting international electronic commerce without unique or identical

[50] Supra (n 48).

definitional frameworks. Electronic commerce's exceptional success will depend more on facilitating and encouraging trade between unknown parties in different jurisdictions than on interactions between known parties, whether within the same jurisdiction or not. The study hereunder examines some of the global, regional and domestic instruments in place to enforce e-signatures.

5.1. United Nations Model Law of Electronic Commerce, 1996

In 1996, the United Nations adopted a Model Law on Electronic Commerce (MLEC) to provide a common policy structure for nations in the drafting of their e-commerce statutes. It is important to note that this was just a guideline and nations had to complement it with comprehensive rules and regulations in order to achieve its implementation. It has had a profound impact on the evolution of international e-commerce law, including definitions, variation by agreement, legal recognition and admissibility of electronic form, incorporation by reference in e-contracts, use of electronic signatures, carriage contracts among others.

The MLEC had many consequences. It approved the use of electronic signatures, claimed that electronic signatures would have the same legal impact as ink signatures and remained technologically neutral, i.e., did not mandate the utilization of any specific type of technology. They also came up with a Model Law on Electronic Signatures (MLES) in 2001 to provide a standard model structure for nations to use when writing their e-signature laws.

The MLES is based on the fundamental principle underpinning Article 7 of the UNCITRAL Model Law on Electronic Commerce with regard to the fulfilment of the signing function in an electronic environment by a technologically neutral approach, which avoids promoting the use of any particular technology or process.

A signature, whether electronic or on paper, is primarily a symbol which signifies intent. Thus, the Standard Commercial Code definition of "signed" includes "any symbol" so long as it is "executed or adopted by a party with the present purpose of authenticating a written document.

Many attempts have been made by the United Nations Commission on International Trade Law to strengthen the quality of these legal rules by adopting model legislation which countries can use as a reference when developing their own legislation. In generating electronic records, the MLEC promotes principles of non-discrimination, technological freedom and functional equivalence. The concept of non-discrimination is at the core. The law ensures that a document is not denied legal meaning, validity or enforceability solely on the grounds that it is in electronic form.

More than 70 nations have embraced the 1996 Model Law on Electronic Commerce (MLEC), and over 30 countries have implemented the 2001 Model Law on Electronic Signatures (MLES). A legally binding treaty was also signed by 18 countries, the 2005 United Nations Convention on the Use of Electronic Media in Foreign Contracts. Regional legal gaps in electronic signature regulations exist for cross-border traders. When states are using the U.N. Model Laws, their respective

governments may choose to implement the elements they like and discard the others. This creates serious uncertainties and makes the system unpredictable.

5.2. United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)

This was adopted on 23 November 2005 and came into force on 1 March 2013. The Electronic Communications Convention aims at facilitating the use of electronic communications in international trade by assuring that contracts concluded and other communications exchanged electronically are as valid and enforceable as their traditional paper-based equivalents.

Certain formal requirements contained in widely adopted international trade law treaties, such as the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the "New York Convention") and the United Nations Convention on Contracts for the International Sale of Goods (CISG) may pose obstacles to the wide use of electronic communications. The Electronic Communications Convention is an enabling treaty whose effect is to remove those formal obstacles by establishing equivalence between electronic and written form. Moreover, the Electronic Communications Convention serves additional purposes further facilitating the use of electronic communications in international trade. Thus, the Convention is intended to strengthen the harmonization of the rules regarding electronic commerce and foster uniformity in the domestic enactment of UNCITRAL model laws relating to electronic commerce, as well as to update and complement certain provisions of those model laws in light of recent practice. Finally, the Convention may provide those countries not having yet adopted provisions on electronic commerce with modern, uniform and carefully drafted legislation.

The Convention builds upon earlier instruments drafted by the Commission, and, in particular, the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures. These instruments are widely considered standard legislative texts setting forth the three fundamental principles of electronic commerce legislation, which the Convention incorporates, namely non-discrimination, technological neutrality and functional equivalence.

The Convention applies to all electronic communications exchanged between parties whose places of business are in different States when at least one party has its place of business in a Contracting State.[51] It may also apply by virtue of the parties' choice. Contracts concluded for personal, family or household purposes, such as those relating to family law and the law of succession, as well as certain financial transactions, negotiable instruments, and documents of title, are excluded from the Convention's scope of application.[52]

As noted above, the Convention sets out criteria for establishing the functional

[51] See Art. 1 of the Convention
[52] *Id.* Art. 2

equivalence between electronic communications and paper documents, as well as between electronic authentication methods and handwritten signatures.[53] Similarly, the Convention defines the time and place of dispatch and receipt of electronic communications, tailoring the traditional rules for these legal concepts to suit the electronic context and innovating with respect to the provisions of the Model Law on Electronic Commerce.[54]

Moreover, the Convention establishes the general principle that communications are not to be denied legal validity solely on the grounds that they were made in electronic form.[55] Specifically, given the proliferation of automated message systems, the Convention allows for the enforceability of contracts entered into by such systems, including when no natural person reviewed the individual actions carried out by them.[56] The Convention further clarifies that a proposal to conclude a contract made through electronic means and not addressed to specific parties amounts to an invitation to deal, rather than an offer whose acceptance binds the offering party, in line with the corresponding provision of the CISG.[57] Moreover, the Convention establishes remedies in case of input errors by natural persons entering information into automated message systems.[58]

Finally, the Convention allows contractual parties to exclude its application or vary its terms within the limits allowed by otherwise applicable legislative provisions (Art. 3).[59] Moreover, States may also consider adopting the provisions of the Convention at the domestic level. Such decision would promote uniformity, economizing on judicial and legislative resources as well as further increasing certainty in commercial transactions, especially in light of the diffusion of mobile devices for electronic transactions. It is particularly recommended for those jurisdictions that have not yet adopted any legislation on electronic commerce. Otherwise, purely domestic communications are not affected by the Convention and will continue to be governed by domestic law.

5.3. Regulation (EU) No 910/2014 of the European Parliament and Council, 2014

This Regulation was passed pursuant to Article 114 of the Treaty on the Functionality of the European Union on 23 July 2014. The Regulation is on electronic identification and trust services for electronic transactions in the internal market and it repealed Directive 1999/93/EC.[60]

The Regulation establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered

[53] *Ibid.* Art. 9
[54] *Ibid.* Art. 10
[55] *Ibid.* Art. 8
[56] *Ibid.* Art. 12
[57] *Ibid.* Art. 11
[58] *Ibid.* Art. 14
[59] *Ibid.* Art. 3
[60] Regulation (EU) No 910/2014 of The European Parliament and of The Council, 2014

delivery services and certificate services for website authentication.[61] The Regulation further gives the legal effect of electronic signatures. Article 25 (1) provides as follows:

> An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.[62]

The regulation also places an electronic signature on the same footing with a handwritten signature. Article 25 (2) provides as follows:

> A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.[63]

The Regulation harmonises the legal position on electronic signatures among all Member states to the European Union. Article 25 (3) provides as follows:

> A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.[64]

This Regulation is very critical in guiding regional, sub-regional and national legislations on e-signatures. It clearly emphasises that an electron signature has the same legal effect with the handwritten signature. It further emphasises that an e-signature shall have the same legal effect with the handwritten signature in all member states under the European Union. The EAC and Uganda in particular can benchmark from this Regulation in enhancing and strengthening their sub-regional and national legislations on e-signatures.

5.4. National Laws

With varying degrees of flexibility, policymakers have used direct regulation, co-regulation, and self-regulation in recent decades to adapt to the growth of global information technology and e-commerce. Different states have signed and ratified various treaties relating to electronic signatures such as the Model Electronic Commerce Act, Model law on Electronic Signatures, the United Nations Convention on the Use of Electronic Communications in International Contracts, among others. Below are some of the countries that have enacted national legislation on electronic signatures.

[61] *Ibid.* Art. 1 (c)
[62] *Ibid.* Art. 25 (1)
[63] *Ibid.* Art. 25 (2)
[64] *Ibid.* Art. 25 (3)

5.4.1. United Kingdom (The Electronic Communications Act 2000)

The Electronic Communications Act 2000 is an important piece of legislation signed into law by the Parliament of the United Kingdom and went into force on March 8, 2002. The ECA has allowed the growth, expansion and use of electronic commerce services in the United Kingdom since then. The primary purpose of the Act was to help build trust in electronic commerce and the technology underlying it by providing businesses and other organizations providing cryptographic support services such as electronic services and confidentiality services with an approval scheme.

5.4.2. Australia (The Electronic Transactions Act 1999)

The Electronic Transactions Act was introduced in 1999. The existing legal provisions prior to 1999 were capable of dealing with electronic transactions but the Electronic Transactions Act 1999 was enacted to provide a more secure environment for e-commerce and the creation of electronic signatures in Australia. By Australian law, contracts are enforceable if the parties have signed the agreement verbally or with a wet-ink (physical) or electronic signature. The law on electronic signatures in Australia is regarded as permissive or minimalist.

5.4.3. New Zealand (Electronic Transactions Act 2002)

The New Zealand Electronic Transactions Act 2002 sets down guidelines for promoting the use of email and other electronic technologies, both in industry and in contact between government and public. In fact, the 2003 Regulation on Electronic Transactions (SR 2003/288) lays down some comprehensive guidelines for different circumstances. On 21 November 2003 the Act and Regulations came into effect.

5.4.4. China (People's Republic of China Electronic Signature Law)

The Electronic Signature Law of the People's Republic of China, published in 2005 and revised in 2015 (the "E-signature Rule") provides legal basis for determining the validity of electronic legislation. Under the law, contracts can be electronically signed. Under Chinese law, a written signature is not necessarily required for a contract to be valid. A contract is valid if parties agree on the terms whether verbally, electronically or in a physical paper document.

5.4.5. European Union (Regulation 910/2014) on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)

The electronic identification and trust services (the eIDAS Regulation) entered into force on 17 September 2014 and was applicable from 1 July 2016. The eIDAS regulation provides a comprehensive legal framework to ensure trustworthiness and legal validity of electronic transactions in the European Single Market. It was meant to provide a predictable regulatory environment for safe and seamless electronic interactions between companies, citizens and public authorities in the European Union. With eIDAS, the EU has succeeded in laying the right foundations and a clear legal framework for citizens, businesses (especially small and medium-sized enterprises) and public administrations to access services securely and make transactions online and across borders in just one click.' Indeed, the roll-out of eIDAS means greater security and convenience for any online e-commerce activity.

5.4.6. Hong Kong (Electronic Transactions Ordinance Act of 2000)

Hong Kong's Electronic Transactions Ordinance provides that contracts cannot be invalidated merely because they were concluded electronically. Under the law, electronic signatures have been recognised as having the same legal status as a wet-ink signature.

6. A REVIEW OF COURT DECISIONS ON THE AUTHENTICITY OF ELECTRONIC SIGNATURES

While not strictly necessary under the rules of evidence, audit trails have proven very effective in authenticating a record to demonstrate that the e-signature is that of the signatory. Courts in different jurisdictions have confirmed this position while in others it is still problematic. This section analyses the different approaches that courts in the United States of America (USA) and the United Kingdom (UK), as a case study, have given to e-signatures.

6.1. Schrock v. Nomac Drilling, LLC, [2016] WL 1181484

In this case, a USA federal court found that detailed e-signature audit logs satisfy the authentication requirement. An employer sought to enforce an electronically signed agreement with a former employee. The court rejected the former employee's challenge to the authenticity of the electronic signature as his own because the employer presented evidence that the e-signature program required the entry of the last four digits of the former employee's social security

number, and the audit trail showed that the document was electronically signed at a specific location at a time when the former employee was at that same location.

6.2. Obi v. Exeter Health Resources, Inc. [2019] WL 2142498

A USA federal district court in New Hampshire rejected the party's argument that her electronic signature on an agreement had been forged, where DocuSign eSignature audit logs showed that she had viewed and signed the agreement through her DocuSign eSignature account.

6.3. Moton v. Maplebear Inc. [2016] WL 616343

A USA district court in the Southern District of New York, found that an e-signature provider's "time-stamped audit trail that tracks using IP addresses and other identifying data when each [signatory] receives, views and executes each agreement" was sufficient to establish that the signer's signature was his own, and that this evidence, in turn, established assent to the agreement.

6.4. IO Moonwalkers, Inc. v. Banc of America, [2018] 814 S.E.2d 583

A DocuSign eSignature audit trail showed that a business accessed a document it claimed it had not signed, which supported the trial court's finding that the business had ratified the signature of the agreement with the other party. There, the party had argued that no one affiliated with his business had signed the agreements at issue and speculated that one of the other party's employees had signed them. However, the evidence showed that the owner of the business had provided the other party with an email address to send agreements for electronic signature, and that the business was familiar with how DocuSign eSignature worked. The DocuSign eSignature audit trail showed that someone with access to the business's email account accessed and then signed the agreements at issue. This audit trail evidence was critical to the court's rejection of the business's effort to create a material dispute of the facts in the case as to whether the agreements at issue had been signed by a representative of its business.

6.5. Harpham v. Big Moose Inspection, [2015] WL 5945842

A USA court found that a more rudimentary audit trail of the party's receipt and electronic signing of agreement was sufficient to overcome the party's unsupported affidavit that he did not recall signing the agreement.

6.6. R v Pusey [1972] Imm AR 240

In this UK case, evidence of the use of an electronic signature was the basis for the court's decision to convict the accused on fraud charges. The defendant, Mr. Pusey, was a former staff director at the Fred Victor Center (the "Center"), a charitable organization based in Toronto. He was also the head of two companies (the "Companies"). These companies billed the Center for more than one hundred thousand dollars for work that was performed by other employees or subcontractors of the Center, in violation of the Center's Code of Conduct regarding Conflicts of Interest. The scheme was discovered when the Center's employees questioned some invoices for payments made to the Companies following the cheque details signed by the accused. As a result, the Center paid out to the Companies various payments totaling more than $115,000 over 16 months. The accused testified that the arrangement was approved by the Center's Executive Director. Allegedly, the scheme was that the Companies billed the Center for work done by subcontractors. Mr. Pusey then paid them in cash to get savings and tax benefits for the Center. The only documentary evidence presented by the accused were contracts allegedly signed by Mr. Pusey (on behalf of the Companies) and the Center's Executive Director. The Center's Executive Director testified that the contracts were fake, and he had refused to sign them. The court examined evidence that the accused's computer and flash drive contained electronic versions of the Executive Director's signature and found that the accused would have had access to the signature. Versions of the electronic signatures on the accused's hard drive were created and modified on the same day, which coincided with the first date when one of the Companies billed the Center. The report of the Center of Forensic Sciences found that the electronic signature and the "contract" signature came from the same signature source "within the limits of practical certainty.". The Judge declared that "the signature on the so-called contract and the electronic signature found on Mr. Pusey's computer are identical." The court rejected Mr. Pusey's explanations and alternative theories when finding him guilty of fraud.

This case demonstrates the legal provability and security problem associated with electronic documents and signatures on negotiable instruments. In most common law jurisdictions, including Ontario, legislation has been in place for many years making the use of electronic signatures legally provable.

The above cases demonstrate that, while audit trails may not be required to authenticate electronic signatures and establish assent to an agreement, they greatly simplify the task of an attorney who must overcome an adversary's claim that he did not sign an agreement or that his e-signature was somehow forged. These cases also reinforce the more general takeaway that an audit trail associated with other types of contracts, such as a clickwrap, also will greatly help in enforcing such contracts. Further, these cases demonstrate that not only does an electronic signature with an audit trail strengthen a party's position, but it also provides no practical downside. Rather than needing to proactively cultivate corroborating

evidence for a challenged paper-and-ink signature, counsel can justifiably rely on an e-signature audit trail to provide heightened substantiation of the authenticity of an electronic document.

7. CHALLENGES ASSOCIATED WITH ELECTRONIC SIGNATURES

In civil evidence, a record or document is regarded as "authentic" if there is evidence that the document or record "is what its proponent claims".[65] The notion of "document" as such is fairly broad and generally encompasses "anything in which information of any description is recorded".[66] This would include, for example, such things as photographs of tombstones and houses,[67] account books[68] and drawings and plans.[69] The relevancy of a document as a piece of evidence is established by connecting it with a person, place or thing, a process which in some common law jurisdictions is known as "authentication".[70] Signing a document is a common albeit not exclusive means of "authentication", and, depending on the context, the terms "to sign" and "to authenticate" may be used as synonyms.[71]

Most legal systems have special procedures or requirements that are intended to enhance the reliability of handwritten signatures. Some procedures may be mandatory in order for certain documents to produce legal effects. They may also be optional and available to parties that wish to act to preclude possible arguments concerning the authenticity of certain documents. Typical examples include the following:

7.1. Notarisation

In certain circumstances, the act of signing has a particular formal significance due to the reinforced trust associated with a special ceremony. This is the case, for instance, with notarization, i.e., the certification by a notary public to establish the

[65] See the USA Federal Rules of Evidence, Rule 901(a):

> The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

[66] United Kingdom of Great Britain and Northern Ireland, Civil Evidence Act 1995, chapter 38, section 13.
[67] Lyell v. Kennedy (No. 3) (1884) 27 Ch.D. 1 (United Kingdom, Chancery Division).
[68] Hayes v. Brown [1920] 1 K.B. 250 (United Kingdom, Law Reports, King's Bench).
[69] J. H. Tucker & Co., Ltd. v. Board of Trade [1955] 2 All ER 522 (United Kingdom, All England Law Reports).
[70] Farm Credit Bank of St. Paul v. William G. Huether, 12 April 1990 (454 N.W.2d 710, 713) (United States, Supreme Court of North Dakota, Northwestern Reporter).
[71] In the context of the revised article 9 of the United States Uniform Commercial Code, for example, "authenticate" is defined as "(A) to sign; or (B) to execute or otherwise adopt a symbol or encrypt or similarly process a record in whole or in part, with the present intent of the authenticating person to identify the person and adopt or accept a record".

authenticity of a signature on a legal document, which often requires the physical appearance of the person before the notary.

7.2. Commissioning

Just like notarisation, commissioning a document requires physical appearance of the deponent before a commissioner of oaths. The rationale is to certify by a commissioner of oaths the authenticity of a signature on a legal document, which often requires the person signing the document to physically appear before the commissioner. This may not be possible under the ESA.

Section 4 of the Commissioner for Oaths (Advocates) Act Cap 5 which provides for the powers of the commissioner and section 5 thereof provides for the particulars to be stated in a jurat or attestation clause in the following words:

> Every commissioner for oaths before whom any oath or affidavit is taken or made under this Act shall state truly in the jurat or attestation at what place and on what date the oath or affidavit is taken or made.[72]

Section 5 of the Act states that:

> Every commissioner for oaths before whom any oath of affidavit is taken or made shall state in the jurat or attestation at what place and on what date the oath or affidavit is taken or made.[73]

Rule 9 of the schedule to the Act provides that the form of the jurat is set out in the third schedule to the rules which requires to state that the oath was sworn and declared before a commissioner for oath in a particular specified place and the date of making it.

Failure to comply with the above requirements, specifically physical presence and writing your signature before the commissioner for oath may render the entire oath defective.[74]

7.3. Attestation

Attestation is the act of watching someone sign a legal document and then signing one's name as a witness. The purpose of attestation is to preserve evidence of the signing. By attesting, the witness states and confirms that the person whom he or she watched sign the document in fact did so. Attesting does not extend to vouching for the accuracy or truthfulness of the document. The witness can be

[72] See Cap. 5, Laws of Uganda
[73] *Id*
[74] See HCMA NO. 31 of 2020, Attorney General vs Okello James Enos & Opolot Edward. High Court of Uganda at Soroti decided on the 02nd day of July 2021.

called on to testify as to the circumstances surrounding the signing.[75]

7.4. Seals

The practice of using seals in addition to, or in substitution of, signatures is not uncommon, especially in certain regions of the world.[76] Signing or sealing may, for example, provide evidence of the identity of the signatory; that the signatory agreed to be bound by the agreement and did so voluntarily; that the document is final and complete; or that the information has not been altered after signing.[77] It may also caution the signatory and indicate the intent to act in a legally binding manner.

7.5. Electronic Print versus Handwritten Print

In *the Matter of an Application for a writ of Habeas Corpus ad subuciendum by Kyagulanyi Sentamu and Another v Attorney General and 2 Others,*[78] the High Court of Uganda was faced with a challenge of determining whether an electronic print of a signature of a deponent on an affidavit as opposed to an original ink print (wet signature) is admissible in evidence or defective. Court noted that it was stated that the affidavit of one of the Respondents was a scanned copy and could not therefore have been sworn before a Commissioner for Oaths and therefore, it is a nullity. In addressing this issue, court made the following observation:

> In resolving this preliminary point, this Court will start with whether the affidavit is a scan and was not therefore signed before a Commissioner for Oaths. I have examined the signature of the affidavit on the court record. It is in black ink and is clearly not an electronic print. It bears an imprint of the pen pressure left when the deponent signed and for that reason the submission that it is a scan is dismissed.[79]

From the above reasoning of court, it appears that the affidavit was simply saved because the Judge was convinced that it was not an electronic print but simply a wet signature. The implication here is that if it was the former, then it would not be saved. The critical concern here is whether the Judge addressed his mind to the provisions of the ESA which were in force at the time of hearing and determining

[75] Adrian McCullagh, Peter Little and William Caelli, "Electronic signatures: understand the past to develop the future", University of New South Wales Law Journal, vol. 21, No. 2 (1998; see chap. III, sect. D, on the concept of witnessing.
[76] Seals are used in several countries in eastern Asia, such as China and Japan.
[77] Mark Sneddon, "Legislating to facilitate electronic signatures and records: exceptions, standards and the impact of the statute book", University of New South Wales Law Journal, vol. 21, No. 2 (1998); see part 2, Chap. II, "Policy objectives of writing and signature requirements".
[78] Miscellaneous Cause 16 of 2021 [2021] UGHCCD 1 (23 January 2021); [2021] UGHCCD 1.
[79] *Id* at pg. 9

this matter.

7.6. The Electronic Signatures Act's Description of the Nature of an Electronic Signature

ESA defines an electronic signature to mean data in electronic form affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message; and includes an advance electronic signature and the secure signature.[80] By implication, it does not need to be a wet signature by electronic.

It further defines an electronic signature product to mean configured hardware or software or relevant components of it, which are intended to be used by a certification service provider for the provision of electronic signature services or are intended to be used for the creation or verification of electronic signatures.[81]

The effect of the above two provisions of the ESA is that such a signature can neither be wet nor made before a notary public, commissioner for oath any other attesting officer under the law. This means that there is still a variance between the ESA and other legislations governing affidavit evidence in Uganda to wit; the Notaries Public Act;[82] the Statutory Declarations Act;[83] the Oaths Act;[84] the Commissioner for Oaths (Advocates) Act;[85] and the Civil Procedure Rules.[86]

7.7. Absence of adequate Public Key Infrastructure

The National Information Technology Authority – Uganda (NITA-U) in April 2022 announced the issuance of Public Key Infrastructure (PKI) license to Pos Digicert. This license and registration cover provision of certification services as well as date & time stamp services.

PoS Digicert, Mantra Technologies and Digital Trust are part of the Joint Venture that was contracted by Government of Uganda to establish and maintain the digital authentication and electronic signatures solution under the brand name UGPASS. This venture supports use of advanced electronic signatures based on trusted and secure PKI. This brought forth for the first time advanced electronic signatures compliant with the ESA and as such admissible in Courts of Law. UGPASS enables users to utilize their existing smart phones to register for a securely verified digital certificates in order to authenticate themselves online for seamless and secure access to a variety of e-services and use advanced electronic

[80] See Section 2 of ESA.
[81] *Id.*
[82] Cap. 18, Laws of Uganda.
[83] Cap. 22, Laws of Uganda.
[84] Cap. 19, Laws of Uganda.
[85] Cap. 5, Laws of Uganda.
[86] S.I. No. 71-1 (as amended by S.I. NO. 33 of 2019)

signatures to securely e-sign documents with the following benefits:

- high level of security;
- high level of user assurance; and
- non-repudiation of User operations.[87]

Notwithstanding the above development, PKI infrastructure is still weak and inadequate in Uganda to control and manage electronic signatures. No wander most public entities still rely on wet signatures and have not embraced electronic signatures in their systems.

Electronic signatures still have challenges in administration of justice in both civil and criminal jurisdictions. We cannot however avoid use of electronic signatures given technological advancement globally. We need to address the shortcomings and make electronic signatures easily admissible in litigation and other court business. The following avenues can help to address some of the above challenges.

8. RECOMMENDATIONS

8.1. Harmonisation of Laws Governing Admissibility of Evidence with the Electronic Signatures Act

This article has demonstrated that the different laws governing affidavit evidence are at variance with the ESA. The Notaries Public Act, the Advocates (Commissioner for Oaths) Act, the Oaths Act, the Statutory Declarations Act and the Civil Procedure Rules are all providing for a wet signature and require the person writing a signature to do so physically in the presence of commissioner for oaths or notaries public. This is not the position with the e-signature which is predominately electronic. There is urgent need to harmonise these pieces of legislation to be in tandem with the ESA.

8.2. Technological Infrastructure Improvement

Technological infrastructure to facilitate e-signature in Uganda is still very weak. Although the NITA-U has licensed a few companies on application of PKI, less application of the system has been realised even in the greater Kampala metropolitan and most public institutions have not yet embraced this technology which makes the system quite inoperative.

[87] **NITA-U Issues First Public Key Infrastructure (PKI) Provider License.** Available at NITA-U Issues First Public Key Infrastructure (PKI) Provider License | National Information Technology Authority - Uganda (NITA-U) https://www.nita.go.ug/nita-u-issues-first-public-key-infrastructure-pki-provider-license (accessed on 14 August 2022)

8.3. Training Efficient and Reliable Human Resource Personnel

This is yet another problem affecting e-signature and e-justice generally in Uganda. ICT is a practical skill which requires experts to run the system. Most legal practitioners representing parties in courts of law, who also prepare affidavits and statutory declarations have little knowledge in ICT. The judiciary has employed some ICT experts like the technical team on Electronic Court Case Management Information System (ECCMIS) who are of ICT background, but they are overwhelmed as they are very few compared to a number of courts in the country and the different stakeholders, they need to serve at a given period of time. Moreover, ECCMIS itself is still challenged by ICT inefficiencies in the country generally. There is need to train legal service providers in ICT to make them relevant and embrace the use of e-signatures.

8.4. Using Passwords and Hybrid Methods to Enhance Security of the Signature

Passwords and codes are used both for controlling access to information or services and for "signing" electronic communications. In practice, the latter use is less frequent than the former, because of the risk of compromising the code if it is transmitted in non-encrypted messages. Passwords and codes are however the most widely used method of "authentication" for purposes of access control and identity verification in a broad range of transactions, including most Internet banking transactions, cash withdrawals at automated teller machines and consumer credit card transactions. It should be recognized that multiple technologies can be used to "authenticate" an electronic transaction. Several technologies or several uses of a single technology can be utilized for a single transaction. For example, signature dynamics for authentication can be combined with cryptography for message integrity. Alternatively, passwords can be sent over the Internet, using cryptography (e.g., SSL in browsers) to protect them, in conjunction with the use of biometrics to trigger a digital signature (asymmetric cryptography), which, on receipt, generates a Kerberos ticket (symmetric cryptography). In developing legal and policy frameworks to deal with these technologies, consideration should be given to the role of multiple technologies. Legal and policy frameworks for electronic authentication will need to be flexible enough to cover hybrid technology approaches, as those that focus on specific technologies could impede the use of multiple technologies.[88] Technology-neutral provisions would facilitate the acceptance of such hybrid technology approaches.

[88] See Foundation for Information Policy Research, Signature Directive Consultation Compilation, 28 October 1998, which provides a compilation of responses made during consultations on the European Union draft directive on electronic signatures, prepared at the request of the European Commission, available at www.fipr.org/publications/sigdirecon.html (accessed on 14 August 2022).

8.5. Licence more Public Key Infrastructure and Certification Services Providers

We appreciate the fact that NITA-U has this year licensed some PKI service providers. We wish however, note the fact that the efforts are still at the infancy stage and need serious boosting. Setting up a PKI is a way to provide confidence that (a) a user's public key has not been changed and in fact corresponds to that user's private key; and (b) the cryptographic techniques being used are sound. To provide such confidence, a PKI may offer a number of services, including the following: (a) managing cryptographic keys used for digital signatures; (b) certifying that a public key corresponds to a private key; (c) providing keys to end-users; (d) publishing revocation information on public keys or certificates; (e) managing personal tokens (e.g. smart cards) that can identify the user with unique personal identification information or can generate and store an individual's private keys; (f) checking the identification of end-users and providing them with services; (g) providing time-stamping services; and (h) managing cryptographic keys used for confidentiality encryption where the use of such a technique is authorized. This with no doubt will increase public confidence in e-signatures as clear safeguards to control their authenticity is in place.

8.6. Using Biometrics to Safeguard Systems

Biometrical devices are generally considered as offering a high level of security. While they are compatible with a range of uses, their current main usage is in government applications, particularly law enforcement applications such as immigration clearance and access controls. Technical solutions might assist in addressing some concerns. For instance, storage of biometrical data on smart cards or tokens may protect against unauthorized access, which could occur if the data is stored on a centralized computer system. Moreover, best practices have been developed to reduce risks in different areas such as scope and capabilities; data protection; user control of personal data; and disclosure, auditing, accountability and oversight.

8.7. Video/Virtual Witnessing of Signatures

Electronic specifically video witnessing of signatures can be adopted. This is very relevant while signing affidavits and statutory declarations. Commissioners for oaths, Notaries Public and Justices of peace can through legislation be permitted to witness a person appending his or her signature on an affidavit electronically by use of video and other relevant gadgets. This can help in dispensing away the requirement of physical presence before such officers.

8.8. Amending Legislation that is Incompatible with Modern Technology

There is urgent need to amend all legislations in force but incompatible with modern technology. All laws should reflect the current technological discourse to remain relevant and facilitate e-justice system. Without this, we shall have e-justice policies without laws to implement them and technological advancements like cyber legislation will be unproductive.

8.9. Training and Sensitising Stakeholders

For e-justice and e-signature to be effectively managed and implemented, it has to be rolled out to all stakeholders including the judiciary, legal practitioners, legislators, academia, training institutions and litigants generally. ICT skills are involved here, and they are not common to everyone. Serious training of staff of the different stakeholders is critical. Early training of students at the university is equally encouraged.

CONCLUSION

Laws that provide for the legal value of digital signatures typically attribute the same legal value to signatures supported by foreign certificates only to the extent that they are regarded as equivalent to domestic certificates. The review done in this study indicates that proper assessment of legal equivalence requires a comparison not only of the technical and security standards attached to a particular signature technology, but also of the rules that would govern the liability of the various parties involved. The UNCITRAL Model Law on Electronic Signatures provides a set of basic common rules governing certain duties of the parties involved in the authentication and signature process that may have an impact on their individual liability. There are also regional texts, such as the European Union directive on electronic signatures, that offer a similar legislative framework for the liability of certification services providers operating in the region. However, neither of those texts addresses all liability issues arising out of the international use of certain electronic authentication and signature methods.

The ESA is already in force but with less application as it seems incompatible with most laws governing evidence in Civil proceedings in Uganda. It is now more than a decade since the Act came into force and has not been fully operationalised as courts to date still accord wet-ink signatures more value than electronic signatures. Electronic signatures globally operate under the principles of non-discrimination, technological neutrality and functional equivalence. We need to quickly revisit our laws governing evidence in civil proceedings to align with the ESA. This will simplify the duty of courts of law while interpreting such laws in cases before them.

IMPACT OF THE CONTINUED USE OF VIDEO CONFERENCING IN COURTS ON THE PRISONER'S RIGHT TO A FAIR TRIAL IN UGANDA

Godfrey Ayeranga*

ABSTRACT

Despite the benefits of using video conferencing in the wake of and post COVID-19, it poses grave challenges to the accused's rights to fair trial since it is hard to read the body language of the accused or witnesses during the virtual sessions, hence difficult to ascertain the credibility of a witness or accused notwithstanding their impact on the outcome of the case. Relatedly, the poor network connections associated with video conferencing affect the quality of the court proceedings which make it difficult to follow either what the accused, lawyers or judicial officer is saying, which may lead to wrong interpretation by either party. The Attorney-client connection is always lacking during video conferencing since some video conferencing tools lack to option to allow for private communications between the accused and their lawyers, yet some prisoners may not be comfortable saying certain statements due to the fear of any repercussions from the prison officers. The author will argue that the continued use of the video conferencing is a continued violation of the accused's right to a fair trial in Uganda.

To analyse the impact of the continued use of the video conferencing on the accused's right to a fair trial in Uganda, the author adopts a desk research methodology that assesses primary sources such as domestic legislation, regional and international law as well as secondary data including the available academic publications, jurisprudence from international human rights bodies and courts, case law from Ugandan courts and reports from media outlets.

* LLB, *Uganda Christian University*; LLM (Human Rights and Democratisation in Africa), *University of Pretoria*, Dip LP, *Kenya School of Law*. Email: ayerangagodfrey@gmail.com. The author acknowledges Mr. Rogers Aheebwa Musiime and Ms. Miriam Lawoko for their insights during the compilation of this paper.

INTRODUCTION

In March 2020, the World Health Organization (WHO) declared the Coronavirus (COVID-19) as a global pandemic and called upon countries to implement measures aimed at containing the virus.[1] On 30 March 2020, the President of the Republic of Uganda, His Excellency Yoweri Kaguta Museveni, declared a nationwide lockdown for a period of fourteen days,[2] which was later extended by another twenty one days in April 2020, and then again in May 2020.[3]

The emergence of COVID-19 placed Ugandan prisoners in a more vulnerable position as they were more susceptible to contract the virus.[4] In a bid to contain the spread of the virus among the prisons, the Chief Justice of Uganda (as he then was), His Lordship Bart Katureebe, issued directives on 19 March 2020 prohibiting the prison authorities from taking prisoners on remand to court and suspending all court hearings and appearances while allowing the use of online hearings for purposes of delivering of judgments and rulings, as well as the hearing of bail applications, mentions and interlocutory applications,[5] a directive that was later extended to 28 May 2020.[6]

The partial closure of the courts implied that prison inmates could not be brought to court yet not all of them could access the video conferencing facilities adopted by the judiciary. Furthermore, conducting some key judicial procedures including plea taking, arraignments, became impossible since all the above court proceedings require the attendance of the accused persons and their lawyers.

2. A SYNOPSIS OF THE ADOPTION OF TECHNOLOGY IN UGANDA'S COURT PROCEEDINGS

On 9 March 2016, the Judiciary launched the Judicature (Visual–Audio Link) Rules, 2016, with specific objectives: to enable courts to easily take evidence in court while using the visual-audio link; to make it easier for witnesses to give

[1] World Health Organisation, 'WHO-Director General's opening remarks at the media briefing on Covid-19 (2020)' <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-bri efing-on-covid-19---11-march-2020> accessed 2 May 2022.

[2] The Observer,'Museveni imposes 14-day COVID-19 lockdown' *The Observer* (Kampala, 30 March 2020) <https://observer.ug/news/headlines/64074-museveni-announces-14-day-covid19-lockdown> accessed 11 May 2022.

[3] Joseph Kiiza,'Uganda relaxes coronavirus lockdown measures' *New Vision* (Kampala, 4 May 2020)<https://www.newvision.co.ug/new_vision/news/1518485/-live-coronavirus-lockdown-ugandas> accessed 3 May 2022.

[4] Toby Cadman, 'COVID-19 Symposium: The Impact of Coronavirus (COVID-19) on Prisoners' (Opinio Juris, 1 April 2020)<https://opiniojuris.org/2020/04/01/covid-19-symposium-the-impact-of-coronavirus-covid-19-on-prisoners/>accessed 2 May 2022.

[5] The Judiciary, 'Chief Justice's Circular, Administrative and Contingency Measures to Prevent and Mitigate the Spread of Corona Virus (Covid-19) By The Judiciary'< https://covidlawlab.org/wp-content/uploads/2021/02/Chief-Justice-Circular-on-COVID-19_recognized-Measures-to-mitigate-the-spread-of-COVID-19-by-the-Judiciary.pdf> accessed 3 May 2022.

[6] The Judiciary, 'Normal Court operations to wait - Chief Justice' <https://www.jlos.go.ug/index.php/document-centre/covid-19/427-press-release-chief-justice-issues-new-covid-19-guidelines-in-regard-to-court-operations-may-28-2020/file> accessed 3 May 2022.

evidence without physically appearing in court; to enable parties to the proceedings including the accused persons, advocates to address court without physically appearing in court; to facilitate speedy trials; to provide for relief from the anxiety of giving evidence in open court; to reduce the cost of litigation; and to promote witness protection.[7] Therefore, the above rules ushered into Ugandan courts the regime of using visual-audio aided technology during the conduct of proceedings.

The above efforts were bolstered in August 2016 when the then Chief Justice of Uganda Bart M. Katureebe launched the Visual-Audio Link as a tool to expedite court processes, reduce case backlog and curb delays in court trials as well as counter the high costs associated with hearing court cases.[8] The Visual-Audio Link refers to giving or receiving of evidence through electronic means without a person physically appearing in court.[9] The installation of the new technology in courts was also aimed at enabling vulnerable witnesses to testify such as the elderly, children and whistle blowers without being in Court, thereby smoothening the process of testimony taking in courts.[10] This technology was first adopted for use in at the Criminal Division of the High Court in Kampala, as well as the High Courts in Fort Portal and Gulu.[11] However, this was not the end as plans of installing such similar facilities in Arua, Mbale, Masindi and Mbarara were being made.[12] It is the above efforts that led to the adoption of the notion of 'Video conferencing' by the Ugandan Courts.

Two years later, after introducing the Visual-Audio Link at the Buganda Road Magistrates' Court, the judiciary launched another video conferencing system at the male wing of Luzira prison in April 2019.[13] At the launch of the Video conferencing system, the then Chief Justice, Bart Katureebe, noted that:

> The system will help improve the work of the Judiciary, Police and Prisons by enabling the court system to handle more hearings in a day in an efficient way as well as reducing the expenditure for prisons, courts and police that play a role in delivering justice.[14]

This was supported by the Commissioner of Prisons, Dr. Johnson Byabashaija, who noted that:

> The video conferencing system would aid in reducing the costs of transporting inmates from prison to courts, improve on the safety and security

[7] Judicature (Visual–Audio Link) Rules, (2016), Rule 4.
[8] The Judiciary, 'CJ Launches Court Audio-Video Link Technology' (The Judiciary, 17 August 2016) <http://www.judiciary.go.ug/data/news/264/CJ%20Launches%20Court%20Audio-Video%20Link%20Technology.html> accessed 5 June 2022.
[9] Derrick Kiyonga, 'Uganda's judicial system: Virtual courts are here but no laws to regulate them' <https://www.unwantedwitness.org/ugandas-judicial-system-virtual-courts-are-here-but-no-laws-to-regulate-them/> accessed 5 June 2022.
[10] Ibid.
[11] The Judiciary(n 9).
[12] Ibid.
[13] Nalubega Petronilla & Joy Aliba, 'Judiciary Launches Video Conferencing System for Luzira Inmates' (Uganda Road Network, 15 April 2019) <https://ugandaradionetwork.net/story/judiciary-launches-video-conferencing-system-for-luzira-inmates?districtId=727> accessed 5 June 2022.
[14] Ibid.

of dangerous inmates and ease access to information during court sessions.[15]

Furthermore, in May 2019, the Chief Justice issued the Constitution (Integration of ICT into the Adjudication Processes for Courts of Judicature) (Practice) Directions, 2019, which further granted the courts powers to use technology in the adjudication of Court cases as the circumstances warrant.[16] Thus, one can rightly say that by 2019, the judiciary had laid a proper foundation for the use of video conferencing in Uganda.

Therefore, it is no surprise that in a bid to contain the spread of the virus among the prisons during the outbreak of COVID-19 in Uganda in March 2020, the judiciary opted for the use of video conferencing technology, by allowing the use of online hearings for purposes of delivering of judgments and rulings, the hearing of bail applications, mentions and interlocutory applications,[17] a directive which was later extended to 28 May 2020.[18] Video Conferencing was successfully adopted by Ugandan courts in 2020,[19] and 2021,[20] during which period some judicial officers praised the video conferencing system for increasing the number of cases being heard by the courts.[21]

However, despite the containment of the COVID-19 scourge, Ugandan courts have continued to used video conferencing systems to date, an issue that both the lawyers and the judiciary have failed to agree on, due to the flaws associated with the use of video conferencing technology such as poor internet connectivity, lack of the necessary infrastructure and equipment required to support the virtual proceedings, among others.[22] Unfortunately, as a result of the above challenges associated with technology, the continued use of video conferencing has led to delays in Court proceedings despite being introduced to reduce delays in court hearings, an issue the author seeks to buttress in this paper while arguing that the continued use of video conferencing technology violates the prisoners' right to a fair trial enshrined in International, regional and national laws of Uganda.

---

[15] Ibid.

[16] Constitution (*Integration of ICT* into The Adjudication *Processes* for *Courts* of Judicature) (Practice) Directions Practice Direction 3.

[17] The Judiciary, 'Chief Justice's Circular, Administrative and Contingency Measures to Prevent and Mitigate the Spread of Corona Virus (Covid-19) By The Judiciary'< https://covidlawlab.org/wp-content/uploads/2021/02/Chief-Justice-Circular-on-COVID-19_recognized-Measures-to-mitigate-the-spread-of-COVID-19-by-the-Judiciary.pdf> accessed 3 May 2022.

[18] The Judiciary, 'Normal Court operations to wait - Chief Justice' <https://www.jlos.go.ug/index.php/document-centre/covid-19/427-press-release-chief-justice-issues-new-covid-19-guidelines-in-regard-to-court-operations-may-28-2020/file> accessed 3 May 2022.

[19] The Judiciary, 'Civil Division Holds First Video Conferencing Case' <http://www.judiciary.go.ug/data/news/898/Civil%20Division%20Holds%20First%20Video%20Conferencing%20Case.html> accessed 3 May 2022.

[20] UNDP, 'Judiciary video conferencing system supported by UNDP eases access to justice in Masaka' 18 July 2021 <https://www.undp.org/uganda/news/judiciary-video-conferencing-system-supported-undp-eases-access-justice-masaka > accessed 3 May 2022.

[21] Ibid

[22] The Independent, 'Lawyers ask judiciary to halt virtual court proceedings citing sluggishness' *The Independent*(Kampala, March 30 2022) <https://www.independent.co.ug/lawyers-ask-judiciary-to-halt-virtual-court-proceedings-citing-sluggishness/> accessed 3 May 2022.

3. A BRIEF SYNOPSIS ON THE RIGHT TO A FAIR TRIAL

The right to a fair trial is at the heart of human rights protection because "without this one right, all the others are at risk."[23] Indeed, an unfair trial can destroy the defendant's liberty, their reputation and lead to the unfair taking away of their life.[24] Indeed, one may argue that the significance of this right maybe the reason why international law does not allow any deviations from the principles of a fair trial.[25]

The right to a fair hearing consists of the following guarantees: equality of arms between the parties to a proceedings; equality of all persons before any judicial body without any distinction whatsoever; adequate opportunity to prepare a case, present arguments and evidence and to challenge or respond to opposing arguments or evidence; the right to consult and be represented by a legal representative or other qualified persons chosen by the party at all stages of the proceedings; the right to the assistance of an interpreter if he or she cannot understand or speak the language used in or by the judicial body; right to a speedy trial and the right to an appeal to a higher judicial body,[26] among others.

However, since the scope of the right to a fair trial is wide, the author will focus on the above elements for purposes of this paper, which are at the risk of being infringed whenever there is resort to the use of video conferencing during court hearings as will be argued later in this paper.

3.1. Normative Content of the Right to a Fair Trial in Uganda

Uganda is a party to international and regional human rights instruments, including inter alia, the Universal Declaration of Human Rights (UDHR),[27] the International Covenant on Civil and Political Rights(ICCPR),[28] the Convention on the rights of the child (CRC),[29] the Convention on the Rights of Persons with Disabilities(CRPD),[30] the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment(CAT),[31] all of which recognise the right to a fair trial, that applies to all persons including prisoners. The above instruments

[23] David Robertson, '*A Dictionary of Human Rights* (2nd edn, Routledge 2004) 86'; Nihal Jayawickrama, '*The Judicial*
Application of Human Rights Law: National, Regional and International Jurisprudence' (2nd edn, Cambridge University Press 2017), 493.
[24] Amal Clooney & Philippa Webb, '*Right to a Fair Trial in International Law'* (Oxford University Press 2021)1
[25] UN Human Rights Committee (HRC), '*General comment no. 32, Article icle 14, Right to equality before courts and tribunals and to fair trial*, 23 August 2007, CCPR/C/GC/32', para 6; UN Human Rights Committee (HRC), '*CCPR General Comment No. 29: Article icle 4: Derogations during a State of Emergency*,' 31 August 2001, CCPR/C/21/Rev.1/Add.11,' para. 11.
[26] The African Commission On Human and Peoples' Rights, 'Principles and Guidelines on the Right to a Fair Trial and Legal Assistance In Africa,' para 2.
[27] UDHR, Article s 10 and 11.
[28] Uganda ratified the ICCPR on 21st June 1995, See Article s 14(1-7).
[29] Uganda ratified the CRC on 17 August 1990, See Article s 12, 40.
[30] Article 13.
[31] Article 15.

impose legal obligations on Uganda to promote access to justice in the field of the criminal justice system, thereby necessitating the promotion and respect for the right to a fair trial in Ugandan courts especially for prison inmates.

3.1.1. International Legal Framework: The Soft Law

(a) Universal Declaration of Human Rights 1948

The Universal Declaration of Human Rights (UDHR) was the first official text to guarantee human rights, which was adopted in 1948. [32] The right to a fair trial was first enshrined in the non-binding declaration and later entrenched in other binding international and regional instruments and national laws of different states including Uganda, as elaborated be in this paper.[33]

Article 10 of the UDHR provides that everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him. This provision guarantees all persons (including prisoners), the right to a fair trial in both civil and criminal proceedings before an independent and impartial tribunal and ensures the promotion of the principle of equality in the enjoyment of the right.[34]

The UDHR recognises the presumption of innocence of all persons charged with a penal offence, and their right to have all the guarantees necessary for his or her defence.[35] This provision stipulates what amounts to a fair trial during criminal proceedings, by guaranteeing the accused an opportunity to prepare his or her defence and the right to a public trial in criminal proceedings. Thus, the UDHR lays a foundation of what amounts to a fair trial in criminal proceedings as explained above.

3.1.2. International Legal Framework: The Hard Law

(a) International Covenant on Civil and Political Rights 1966

The International Covenant on Civil and Political Rights (ICCPR) guarantees the accused's right to a fair and public hearing before a competent, independent and impartial tribunal established by law; the right to be equal before the courts of law and to be presumed innocent during a criminal

[32] Nakibuule Gladys Kisekka, 'Plea bargaining as a human rights question' (2020) 6:1 Cogent Social Sciences <https://www.tandfonline.com/doi/pdf/10.1080/23311886.2020.1818935?needAccess=true> accessed 18 May 2022.
[33] Ibid.
[34] David Weissbrodt & Mattias Hallendorff, 'Travaux Preparatoires of the Fair Trial Provisions--Articles 8 to 11--of the Universal Declaration of Human Rights' (1999) 21 Human Rights Quarterly <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1417&context=faculty_articles> accessed 18 May 2022.
[35] Article 11.

proceeding.[36] The Human Rights Committee(HRC) has noted that Article 14 of the ICCPR guarantees a series of rights including the right to equality before the courts and tribunals and to a fair trial which play a key role in human rights protection and serves as a procedural means to safeguard the rule of law.[37]

The ICCPR contains the minimum procedural rights an accused person is entitled to when undergoing a criminal trial. These include the right to be presumed innocent;[38] the right to be informed of the nature of the charge being faced promptly in a language which he understands;[39] right to have adequate time and facilities to prepare his defence and to communicate with counsel of his own choosing;[40] right to be tried without undue delay;[41] right to be present during trial, to defend himself and to legal assistance either of his own choosing; and to have legal assistance assigned to him, in any case where the interests of justice so require;[42] right to examine and call witnesses during trial;[43] right to have the free assistance of an interpreter,[44] and the right not to be compelled to testify against himself or to confess guilt.[45]

The Human Rights Committee has noted that Article 14 contains guarantees that states, including Uganda must respect, regardless of their domestic law. This places a duty on states, Uganda inclusive to uphold the right to a fair trial of accused persons during criminal proceedings.[46]

(b) Convention on the Rights of the Child 1989

Article 37(d) of the Convention on the Rights of the Child (CRC) recognises the right of every child deprived of his or her liberty to prompt access to legal and other appropriate assistance, and the right to challenge the legality of the deprivation of his or her liberty before a court or other competent, independent and impartial authority, and to a prompt decision on any such action.

The CRC also guarantees every child deprived of his or her liberty the right to maintain contact with his or her family through correspondence and visits, except in exceptional circumstances.[47]

It also recognises other free trial elements such as the right to assistance of an interpreter,[48] the right to appeal against the decision by which he is found guilty of the charge(s) brought against him/her;[49] the right to be presumed innocence for children in conflict with the law;[50] the right to be provided legal or other

[36] Article 14(1) & (2).
[37] UN Human Rights Committee (HRC), *General Comment no. 32* (n 26) 2.
[38] Article (14)2.
[39] Article (14)3(a).
[40] Article (14)3(b).
[41] Article (14)3(c).
[42] Article (14)3(d).
[43] Article (14)3(e).
[44] Article (14)3(f).
[45] Article (14)3(g).
[46] UN Human Rights Committee (HRC), *General Comment no. 32* (n 26) 4.
[47] Article 37(c).
[48] Article 40 (2) (vi).
[49] Article 40 (2) (b) (v).
[50] Article 40(2) (b).

appropriate assistance in the preparation and presentation of his/her defence ;[51] right to be informed promptly and directly of the charges against him or her;[52] the right be heard in any judicial and administrative proceedings affecting the child.[53] The UN Committee on the rights of the child(CRC Committee) has noted that the right to be heard is fundamental for a fair trial, and it must be fully observed throughout the entire juvenile justice process starting from the pretrial stage, during the adjudication and of implementation of the imposed measures.[54] Therefore, the child must be able to express his/her views freely and their views must be given due weight depending on the age and maturity of the child.[55]

The CRC also obliges states to ensure that cases dealing with children in conflict with the law are handled without delay.[56] The CRC Committee has recommended that the States must set and ensure that the period between the commission of the offence and the completion of the police investigation, the decision of the prosecutor (or other competent body) to bring charges against the child, and the timelines for final adjudication and decision by the court or other competent judicial body is shorter than those set for adults.[57]

(c) Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment

Article 15 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT) prohibits the use of any evidence obtained by torture during criminal proceedings, whether in the form of witness statements or confessions. This provision protects the right to a fair trial since any admission of such evidence violates the accused's right to a fair trial.

The UN Special rapporteur of on torture and other cruel, inhuman or degrading treatment or punishment, Juan E. Méndez has noted that, 'confessions and other information extracted under torture or ill-treatment are not considered reliable enough as a source of evidence in any legal proceeding and their admission violates the rights of due process and a fair trial,[58] a position been re-echoed by the UN Committee against Torture.[59] The Special rapporteur further noted that, ' the inadmissibility of unlawfully obtained confessions and other tainted evidence is not only one of the essential means of preventing torture and other ill-treatment, but is also crucial to guarantees of a fair trial.'[60] Therefore, the Article 15 of the CAT upholds fair trial rights of accused persons.

---

[51] Article 40(2)(b) (ii).
[52] Ibid.
[53] Article 12(2).
[54] UN Committee on the Rights of the Child (CRC), *General comment No. 10 (2007): Children's Rights in Juvenile Justice*, 25 April 2007, CRC/C/GC/10, Para 44.
[55] Ibid
[56] Article 40 (2) (b) (iii).
[57] UN Committee on the Rights of the Child (n 55) para 47.
[58] UN Human Rights Council, 'UN Special rapporteur of on torture and other cruel, inhuman or degrading treatment or punishment, Juan E. Méndez' A/HRC/25/60, para 21.
[59] UN Committee against Torture, General *Comment No. 2: Implementation of Article 2 by States Parties*, 24 January 2008, CAT/C/GC/2, para. 6.
[60] UN Special rapporteur of on torture (n 59) para 64.

3.1.3. Regional Framework

(a) African Charter on Human and Peoples' Rights

Article 7 of the African Charter on Human and Peoples' Rights (the African Charter) provides for the right to a fair trial and stipulates as follows:

1. Every individual shall have the right to have his cause heard. This comprises:
   a) the right to an appeal to competent national organs against acts of violating his fundamental rights as recognized and guaranteed by conventions, laws, regulations and customs in force;
   b) (b) the right to be presumed innocent until proved guilty by a competent court or tribunal;
   c) the right to defence, including the right to be defended by counsel of his choice;
   d) (d) the right to be tried within a reasonable time by an impartial court or tribunal.
2. No one may be condemned for an act or omission which did not constitute a legally punishable offence at the time it was committed. No penalty may be inflicted for an offence for which no provision was made at the time it was committed. Punishment is personal and can be imposed only on the offender.

Therefore, Article 7 recognises the accused's right to be heard and the right to defence,[61] the right to legal assistance,[62] the right to be tried within a reasonable time,[63] right to be presumed innocent,[64] all of which constitute the tenets of the right to a fair trial. The African Court on Human and Peoples' rights has noted that right to a fair trial under Article 7 is non-derogable "regardless of the prevailing situation occurring in the state party to the African Charter."[65]

Article 7 is not exhaustive of the elements of the right to a fair trial, which explains why the African Commission on Human and Peoples' Rights expounded on the scope of Article 7 in the 1992 Resolution on the "Right to Recourse Procedure and Fair Trial.[66] The resolution highlights the other components of the fair trial guarantees to include: the right to equality before courts and tribunals and

[61] *Alex Thomas v. Tanzania*, Application No. 005/2013, Judgment of 20 November 2015, para.181
[62] Ibid, para. 123.
[63] *Wilfred Onyango Nganya and 9 Others v. Tanzania*, Application No. 006/2013, Judgment of 18 March 2016, *para 127*
[64] *Mohamed Abubakari v. Tanzania*, Application No. 007/2013, Judgment of 3 June 2016, para. 174
[65] *African Commission on Human and Peoples' Rights v. Libya*, Application No. 002/2013, Judgment of 3 June 2016, paras. 76-77.
[66] African Commission on Human and Peoples' Rights, 'Resolution on the Right to Recourse Procedures and Fair Trial,' 11th ordinary session of the African Commission on Human and Peoples' Rights, Tunis, Tunisia, 2-9 March 1992.

to be heard; to be promptly informed the reasons for the arrest and charges; the right to be presumed innocent; to prepare the defence; to be tried within a reasonable time; examine witnesses and the free assistance of an interpreter; right to appeal to a higher Court.[67]

Although the African Charter does not specifically provide for the right to legal aid,[68] yet the African Commission has found that the right to legal aid is a key component of the right to a fair hearing.[69] This right can be found in a number of Declarations including but to limited to the Dakar Declaration,[70] and the Lilongwe Declaration which require the states to recognize and support the right to legal aid in their criminal justice systems.[71]

Other International and regional rules governing the standards of a fair trial, which prisoners are entitled to include; the Principles and Guidelines on the Right to a Fair Trial and Legal Assistance in Africa which provide that in the determination of any criminal charge against a person, or of a person's rights and obligations, everyone shall be entitled to a fair and public hearing by a legally constituted competent, independent and impartial judicial body.[72]

3.1.4. National Legal Framework

The government of Uganda has passed and adopted policies and regulations aimed at promoting the right to a fair trial in criminal proceedings across the country.

(a) The 1995 Constitution of the Republic of Uganda

The 1995 Constitution of the Republic of Uganda, as amended (the Constitution), which is the supreme law of the law, contains provisions that recognise the right to a fair hearing and its associated rights including the right to be given adequate time and facilities to prepare his or her defence;[73] the right to apply for bail;[74] the rule against double jeopardy;[75] right to an interpreter where the accused person cannot understand the language used at the trial;[76] right to legal representation;[77] and the right to examine witnesses and to obtain the attendance of other witnesses before the court.[78] The Constitution prohibits any derogation from

[67] Para 2(a-i) and para 3
[68] *Alex Thomas* (n 62)144
[69] Dakar Declaration; ACI-IPR /Res.4l(XXVI)99: Resolution on the Right to a fair Hearing and Legal Aid in Africa (1996)
[70] Ibid, para 9
[71] Lilongwe Declaration on Accessing Legal Aid in the Criminal Justice System in Africa, Conference on Legal Aid in Criminal Justice: the Role of Lawyers, Non- Lawyers and other service Providers in Africa, Lilongwe, Malawi, November 22-24, 2004.
[72] Principle 1
[73] Article 28(3)(c)
[74] Article 23(6)(a) and (b)
[75] Article 28(9) and (10)
[76] Article 28 (3)(f)
[77] Article 28(3)(e)
[78] Article 28(3)(g)

the right to a fair hearing.[79]

(b) The Judicature Act Cap 13

Section 18 of the Judicature Act obligates judges of the High Court to sit continuously as reasonably practicable for purposes of determining both civil and criminal cases depending on the nature of the matters to be disposed of subject to the Court vacations. Furthermore, under Section 17(2) g of the act, the High Court has powers to discontinue any delayed prosecutions and to make orders aimed at expediting court trials so as to curb delays, in trials.

Under Section 19(2) of the Judicature Act, High Court circuits are established through which the High Court holds sessions in various areas of Uganda for purposes of hearing both criminal and civil matters pending at such a time and place, thereby reducing case backlog.

Thus, the above provisions of the Judicature act guarantee the right to a speedy trial, which is one of the tenets of the right to a fair trial.

(c) The Magistrates Court Act Cap 16

The Magistrates Act prohibits the punishment of a person twice for the same offence,[80] and provides that, any person accused appearing before a magistrate's court has the right be defended by an advocate.[81] The above provisions uphold the rule against double jeopardy and the accused's right to defend himself and to legal representation, all of which are components of the right to a fair trial.

(d) The Criminal Procedure Code Act Cap 116

Section 48 of the Criminal Procedure Code Act grants the High Court supervisory powers that allow the High Court to call for and examine the record of any criminal proceedings before any magistrate's court for the purpose of satisfying itself as to the correctness, legality or propriety of any finding, sentence or order recorded or passed, and as to the regularity of any proceedings of the magistrate's court. The act also provides for the accused's right of bail pending appeal;[82] and the right of appeal.[83] This legislation is an important tool in upholding the accused's right to a fair trial in Uganda since it recognises some of the key elements of the principle of fair hearing.

(e) Trial on Indictment Act Cap 23

Section 14(1) Trial on Indictments Act (TIA) provides that the High Court may at any stage in the proceedings release the accused person on bail. This provision

[79] Article 44(c)
[80] Magistrates Court act, Section 18.
[81] Ibid, Section 158
[82] Criminal Procedure Code Act, Section 40(2); 47
[83] Ibid, Section 28(4)

protects the accused's right to bail, thereby promoting the principle of the presumption of innocence of an accused which is one of the elements of the right to a fair trial.

However, Section 14(2) TIA contains a clawback clause that grants power to the High Court to deny an accused bail, where he or she does not prove to the satisfaction of the court that exceptional circumstances exist justifying his or her release on bail; and that he or she will not abscond when released on bail. Therefore, the above provision hinders the enjoyment of the right to a fair trial in criminal proceedings in Uganda.

(f) The Children Act Cap 59

Section 99(1) of the Children Act, as amended, requires the courts to handle the cases dealing with children in conflict with the law expeditiously. This provision is operationalized by Section 99(2) of the same act which sets a period of three or twelve months depending on the seriousness of the case within which a case may be heard, or else the case will be dismissed, and the child is protected from further prosecution related to the case. The Act also recognises the right to bail,[84] which is a key component of the right to a fair hearing. Therefore, the right to a fair trial of juveniles is guaranteed under the above provisions.

4. IMPACT OF THE CONTINUED USE OF VIDEO CONFERENCING ON THE PRISONER'S RIGHT TO A FAIR TRIAL

In *Soon Yeon Kong Kim and Anor vs Attorney General*,[85] Mpagi Bahigeine, JA (as she then was), while highlighting the importance of a fair trial, cited with approval the following passage from the Kenyan Constitutional Court case of *Juma and others vs Attorney General:*[86]

> The accused must be given and afforded those opportunities and means so that the prosecution does not gain an undeserved or unfair advantage over the accused; and the accused is not impeded in any manner and does not suffer unfair disadvantage and prejudice in preparing his defence, confronting his accusers and arming himself in his defence and so that no miscarriage of justice is occasioned.[87]

The above statement implies that for a trial to be termed "a fair trial," the accused must not suffer any prejudice or unfair disadvantage during the course of the court trial, that would affect either their defence or preparation of their defence.

However, in this section, the author argues that the achieving the above becomes illusory due to the flaws of video conferencing as discussed below.

[84] Children Act, Sections 88 and 108.
[85] Constitutional Reference No. 6 of 2007.
[86] Kenya (2003) 2 EA 461.
[87] Supra (n 86) 6.

4.1. Video Conferencing Inhibits the Accused's Right to Effectively Participate in Court Proceedings

Article 28(5) of the Constitution stipulates that the trial of any person shall not take place in the absence of that person except where their physical attendance becomes impracticable. Similarly, the ICCPR stipulates that that everyone charged of a criminal offence has a right to be in his presence.[88] The above provisions emphasise the accused's right to be tried in his or her Presence. The Human Rights Committee has noted that the right to a fair trial requires that accused persons be present during their trial.[89] Thus, the accused must be present at all stages of the proceedings. Therefore, the accused's attendance and participation in court proceedings is of paramount importance to the accused since the accused is at the centre of the trial process as the person whose liberty and right to life are at stake.[90] In *Sakhnovskiy v. Russia*,[91] the European Court of Human Rights Court held that resorting to a video hearing is a restriction of the right to be present and called upon states to ensure that the arrangements for giving evidence comply with requirements for due process.

However, due to the challenges associated with video conferencing including poor internet connectivity leading to poor quality of video and audio output, the accused is unable to clearly follow the proceedings and to speak with their counsel.[92] In March 2022, Andrew Koluo, the Toroma County MP, noted that:

> Video conferencing has at times been affected by poor network connections which disrupt and distort court proceedings, and … sometimes the accused end up mentioning things they do not understand, and they are victimized for that simply because they have not heard what the judge or magistrate is asking them due to poor network.[93]

The above concern illustrates how the continued use of video conferencing hampers the accused's right to a fair trial as they are unable to effectively participate in and follow the Court proceedings, as they become disengaged in the process of the trial and are cut-off from the process,[94] due to the challenges caused by video conferencing system which in the long run affects the outcome of their case.

---

[88] Article 14(3) d

[89] UN Human Rights Committee (HRC), *General Comment no. 32*, Para 36

[90] Sahana Manjesh & Madhurima Dhanuka, 'Disconnected Videoconferencing and Fair Trial Rights' Commonwealth Human Rights Initiative(CHRI 2020) 36

[91] ECtHR 2 November 2010, no. 21272/03

[92] Sahana(n 89)18

[93] The Independent, 'MPs divided over continued use of video conferencing in courts' Thr Independent(Kampala, March 14 2022)<https://www.independent.co.ug/mps-divided-over-continued-use-of-video-conferencing-in-courts/>accessed 5 June 2022

[94] Carolyn McKay, (2016), "Video Links from the Prison: Permeability and the Carceral World" 5(1) I*nternational Journal for Crime, Justice and Social Democracy 2016* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937479> accessed 6 June

4.2. Video Conferencing Violates the Accused's Right to a Speedy Trial

The ICCPR requires an accused person charged of a criminal offence to be tried without undue delay.[95] Furthermore, Article 28(1) of the Constitution provides that:

> In the determination of civil rights and obligations or any criminal charge, a person shall be entitled to a fair, speedy and public hearing before an independent and impartial court or tribunal established by law.

In *Kanyamunyu Mathew v Uganda,*[96] Mubiru J noted that:

> Article 28 (1) of the Constitution of the Republic of Uganda, 1995 guarantees to each person accused of an offence, a fair, speedy and public hearing before an independent and impartial court established by law …. The most important right of the criminally accused is the right to a fair trial. Derogation from the enjoyment of this right is constitutionally prohibited … The guarantee relates not only to the time by which a trial should commence, but also the time by which it should end and judgment be rendered; all stages must take place in a "speedy" manner … One aspect of a fair trial is the taking of reasonable steps to prevent avoidable delay so as to guarantee a speedy hearing."

The Human Rights Committee has noted that the right to a fair hearing consists of the right to be heard within a reasonable time,[97] and without undue delay which relates not only to the time between the formal charging of the accused and the time by which a trial should commence, but also the time until the final judgement on appeal.[98] Failure to hear the accused's case within a reasonable time makes the criminal proceedings unfair, thereby violating the accused's right to a fair hearing.

However, the continued use of video conferencing hinders the enjoyment of the accused's right to a speedy trial since video conferencing is associated with problems such as poor internet connectivity which lead to poor quality output of the video and audio from the video conferencing system, that makes it hard for the accused to clearly follow the proceedings. This in the long run causes delay in the court proceedings especially where the video conferencing system either becomes faulty or due to poor internet connectivity, the court sessions are unable to continue or prolonged as attempts are made to restore the non- responsive system.

The courts in Uganda have encountered the above challenges on numerous occasions. For example, in October 2021, it was reported that over 100 cases had been delayed for over three months due to poor Internet link up between Luweero court and premier detention facilities at both Kitalya and Kigo government prisons in Wakiso District, outside Kampala.[99] Similarly, in March 2022, some Ugandan

[95] Article 14(3) c
[96] Criminal Miscellaneous Application 151 of 2020) [2020] UGHCCRD 144 (09 November 2020)
[97] UN Human Rights Committee, Fei v. Colombia, Communication No. 514/1992, UN Doc CCPR/C/53/D/514/1992 (1995), para. 8.4
[98] UN Human Rights Committee, Communication No. 1089/2002, Rouse v. Philippines, para.7.4
[99] Daily Monitor 'Quickly fix gaps in e-court cases' *Daily Monitor* (Kampala, 13 October 2021), <https://www.monitor.co.ug/uganda/oped/editorial/quickly-fix-gaps-in-e-court-cases-3581420>

defence lawyers decried that, constant communication between the suspects in prisons and courtrooms is hard due to the continuous poor internet connectivity, while others have noted that the video conferencing system oftentimes fails and the court sessions are made to wait longer than they would take on travel, thereby losing a lot of precious time in the process of fidgeting with the less responsive system.[100]

4.3. Video Conferencing Violates the Accused's Right of Defence During the Trial

Under Article 14(3) of the ICCPR, the right to a fair includes the accused's right to have adequate time and facilities for the preparation of his defence and to communicate with counsel of his own choosing. The Human Rights Committee has noted that this provision is an important element of the guarantee of a fair trial.[101] It has further noted that the right to communicate with counsel requires that the accused is granted prompt access to counsel who should be to meet their clients in private and to communicate with the accused in conditions that fully respect the confidentiality of their communications without restrictions, influence, pressure or undue interference.[102] Article 14(3) of the ICCPR seeks to emphasise the important role lawyers play in the protection of the right to a fair trial and liberty among others.[103] Unfortunately, video conferencing systems deny the lawyers an opportunity to carry out their duties effectively as it becomes hard for the lawyer to consult with the accused regarding any important decisions to be made during the trial as well as communicating with the defendant about the case before or during the trial yet Counsel representing a defendant in a criminal proceeding must advocate for her client's cause, consult with the defendant about critical decisions, and communicate with the defendant about the case.[104]

The above defect of video conferencing was recently brought to the forefront when, in May 2019, one of the lawyers representing a defendant during the virtual hearing of a bail application, noted that video conferencing system hinders clients from consulting their lawyers (and lawyers from conferring with their clients) while court is proceeding.[105] As such, the standard highlighted above from the decision of Mpagi Bahigeine JA (as she then was) in *Soon Yeon Kong Kim and Anor vs Attorney General* is impossible to achieve when trials are conducted through video conferencing, because of the inherent limitations of that technology.

Relatedly, the use of video conferencing in criminal proceedings makes it hard for the defence lawyers to effectively communicate in a confidential manner with the accused and vice versa due to the disconnect created between the two with the

accessed 6 June 2022.

[100] The Independent, 'Lawyers ask judiciary to halt virtual court proceedings citing sluggishness' *The Independent* (Kampala, 30 March 2022), <https://www.independent.co.ug/lawyers-ask-judiciary-to-halt-virtual-court-proceedings-citing-sluggishness/ > accessed 6 June 2022.

[101] UN Human Rights Committee (HRC), General Comment no. 32, Para 32.

[102] Communications No. 1117/2002 *Khomidova v. Tajikistan*, para. 6.4.

[103] International Commission of Jurists, Videoconferencing, Courts and COVID-19 Recommendations Based on International Standards (International Commission of Jurists, 2020)14

[104] Strickland v. Washington, 466 U.S. 668.

[105] The Independent, 'Mixed reactions over use of video conferencing at Bobi Wine's bail hearing', The Independent(3 May 2019) <https://www.independent.co.ug/mixed-reactions-over-use-of-video-conferencing-at-bobi-wines-bail-hearing/> accessed 7 June 2022.

lawyer appearing in court alone while the accused attends the court proceedings from prison or the detention facility.[106] Therefore, not being in the same room makes the exchange of information, pre-trial and post-trial consultations between the accused and their lawyer hard and further makes it difficult for the lawyer to provide any emotional support to a defendant who appears via screen.[107] Hence, the continued use of video conferencing in criminal proceedings is a violation of the accused's rights of access to defence counsel and confidentiality as the accused do not always have access to their lawyers during Court hearings,[108] as would have been with physical court hearings.

Related to the above, video conferencing violates the accused's right to interface with witnesses contrary to Article 14(3)(e) of the ICCPR which grants the accused the right to examine, or have examined, the witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him. The Human Rights Committee has noted that the above provision aids the accused and their counsel to have an effective defence and grants the accused the same legal powers of compelling the attendance of witnesses and of examining or cross-examining any witnesses as are available to the prosecution.[109]

The Human Rights Committee has further noted that Article 14(3) e grants that accused only a right to have witnesses admitted that are relevant for the defence, and to be given a proper opportunity to question and challenge witnesses against them at some stage of the proceedings.[110] Therefore, the above provision enables the accused to challenge the witness testimony of the prosecution while granting him or her the chance to call his own witnesses that would assist him to establish their defence.

Although the author agrees with Nanima who argues that video conferencing offers a facility that allows for the reception of evidence without their physical presence in court and enables the accused to examine witnesses and obtain the attendance of other witnesses using the video conferencing technology within the meaning of Article 28(3)(g) of the Constitution. [111] However, it is important to note that the Judicature (Visual–Audio Link) Rules, 2016, that permit the use of video conferencing during criminal proceedings can only be used by a few magistrates' courts in the country and are the technology is only placed in designated places with the Court, thereby ignoring the cases before the High Court which in the long run leads to case backlog and violates the right to a fair trial.[112] Furthermore, examination of witnesses may turn out to be a challenge due to the poor internet connectivity and limited access to the video conferencing machinery, hence

[106] Sahana(n 89)19.

[107] Dorris De Vocht 'Trials by video link after the pandemic: the pros and cons of the expansion of virtual justice' (2020)China-EU Law Journal < https://www.ncbi.nlm.nih.gov/pmc/Article icles/PMC9007046/pdf/12689_2022_Article icle_95.pdf/?tool=EBI> accessed 7 June 2022

[108] Sahana(n 89).

[109] UN Human Rights Committee (HRC), *General Comment no. 32*, Para 39.

[110] Ibid.

[111] Robert Doya Nanima, 'A right to a fair trial in Uganda's Judicature (Visual-Audio Link) Rules: embracing the challenges in the era of Covid-19,' (2020) 46:3 Commonwealth Law Bulletin < https://www.tandfonline.com/doi/pdf/10.1080/03050718.2020.1804419?needAccess=true> accessed 20 June 2022.

[112] Ibid, 409.

violating the right to a fair trial. In any event, it is also difficult to read the demeanour of the witnesses due to the barriers created by technology, yet it plays a key role in determining the outcome of the case.

4.4. Video Conferencing Violates the Right to Equity of Arms of an Accused Person

Article 14(1) of the ICCPR requires all persons to be treated equally before the courts and tribunals. The Human Rights Committee in its General Comment No 32, has noted that equity of arms is a key component of the right to a fair trial which ensures that the parties to the proceedings in question are treated without any discrimination.[113] Unfortunately, video conferencing promotes inequalities between the parties to the criminal proceedings since participation in video conferencing hearings requires the users to possess the necessary knowledge to operate the video conferencing technology, and the parties must have access to good quality gadgets such as laptops, mobile phones or computers and internet connectivity.[114] Furthermore, the state tends to have an upper hand in determining how and when the accused will be produced in Court and the timelines for the court appearances are dictated by the state that own the video conferencing systems,[115] thereby placing the accused person and their lawyer at a disadvantage hence a violation of Article 14(1) of the ICCPR. Based on the above, some lawyers may face technical difficulties during the conduct of video conferencing hearings, which in the long run violates their right to a fair hearing.

4.5. Video Conferencing Violates the Accused's Right to a Public Hearing

The ICCPR provides that everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law.[116] Open court proceedings promote public trust in the justice system, act as a mechanism of checking arbitrary judicial actions,[117] and enable the accused's friends and family to follow the accused case.[118]

Although the accused's trial ought to be conducted before a public hearing pursuant to the international standards of a fair trial, video conferenced hearings can be termed as closed hearings because attendance is limited to only specific persons invited by the Court as members of the public are blocked out from attending the court hearings, while some virtual platforms such as Zoom, Google Meet being used to conduct the virtual hearings do not allow multiple users.[119] Therefore, since a majority of the videoconferencing hearings do not allow all the interested friends and family and general public access to the proceedings with

[113] UN Human Rights Committee (HRC), *General Comment no. 32*, Para 8.
[114] Sahana (n 89) 23.
[115] Ibid.
[116] Article 14(1).
[117] Penelope Gibbs, 'Defendants on Video: Conveyor Belt Justice or a Revolution in Access?: Transform Justice' (October 2017) https://www.transformjustice.org.uk/wp-content/uploads/2017/10/Disconnected-Thumbnail-2.pdf> accessed 5 June 2022.
[118] Sahana (n 89) 22.
[119] Ibid.

access being limited to a few by court, this amounts to a violation of the accused's right to a public trial during criminal proceedings.

CONCLUSION AND RECOMMENDATIONS

This article has shown that despite the benefits of video conferencing technology during the conduct of criminal proceedings including but not limited to enabling the conduct of quick court hearings, reducing the transportation costs associated with the transportation of the prisoners as the prisoners do not need to attend the court proceedings in person, as well as promoting security of the witnesses and prisoners, the author argues that Courts and the other stakeholders involved in the criminal justice system ought to be cautious before rushing to fully embrace virtual court proceedings as this study has shown that they violate the right to a fair trial as elaborated in this paper. Therefore, as courts continue to adopt the use of video conferencing systems, there is need for consultative engagements between the government and the other legal service providers especially the defence lawyers, prosecutors among other stakeholders involved in the promotion of access to justice in Uganda.

However, courts can uphold the accused's right to a fair trial by undertaking the following measures during the conduct of video conferencing proceedings:

- All Virtual proceedings must be kept open to the public except when special circumstances warrant. This can be through the simultaneous broadcasting of the court proceedings or allowing access to the video feed upon application by interested individual members of the public.[120] This would play a key role in ensuring that the accused's right to an open court hearing is upheld by enabling the friends and family of the accused keep track of his or her case.
- In a bid to promote Advocate-client confidentiality during video conference hearings, courts must facilitate and permit private communication between the lawyer and accused. This can be achieved through creating and adopting the use of technology that enables the use of breakout rooms' features on the video conferencing systems for purposes of enabling the lawyer and accused to have private communication before, during and after the court proceedings. Similarly, the judge should permit the defence lawyer to always seek permission to speak to the accused in private whenever the need arises, and special rooms and facilities must be created both at detention facilities and courts to allow the accused and their lawyer to easily communicate confidentially.[121]
- To ensure the effective participation of the accused in the video conferencing proceedings, the accused person(s)must be trained on how to use the video conferencing system prior to the start of the trial either by the judge, the prison authorities, or their lawyer(s).
- Related to the above, Court must ensure that the accused is visible to the Court and the accused can see the parties involved in the matter; the visual-audio system is tested and functional prior to the court hearings and that the accused's visual-audio system is functional during the course of the court proceedings. This will ensure that the accused clearly follows

[120] International Commission of Jurists*(n 102)*,16
[121] Ibid.

the court proceedings, thereby promoting the effective participation of the accused in the court proceedings. Similarly, the Court must ensure that there are always technical personnel to assist all the parties to the proceedings in case need arises during the course of the proceedings.

- There is need for the conduct of more periodic trainings for the technical staff operating the video conferencing system, judicial officers, defence lawyers, the prosecutors and the police officers, who are all involved in the administration of justice in courts. This will ensure that the above persons uphold the accused's right to a fair trial during the conduct of the proceedings as they would ensure that the proceedings are in tandem with the fair trial principles discussed above.
- In order to aid the accused to prepare their defence and to fully participate in the proceedings, the judge must ensure that all the court documents, which the judge or parties intend to rely upon during the court proceedings, are sent to the accused prior to start of the hearing.
- Prison authorities must ensure that each prison facility is well equipped with a computer connected with high-speed internet connectivity should be available.
- Furthermore, there is need for amendment of the existing rules governing virtual court so as to address the limitations caused by video conferencing technology hearings raised by the author in this paper. The amendment can be followed by the adoption of new regulations that seek to fill the gaps associated with video conferencing technology. For example, the rules can adopt a hybrid mode of hearing the court cases by making an allowance for the conduct of some physical hearings during the key stages of the trial especially at the pretrial stage, the hearing of the main case especially the hearing of the witness testimony and at the end of the criminal trial.
- Related to the above, the new rules should grant every presiding judicial officer the discretion to discontinue any proceedings in the event that the court faces technical challenges during the court hearing that would make the hearing unfair (non-compliant with the fair trial principles associated with the right to a fair trial) or where an issue that warrants the defendant's personal appearance in the court arises during the virtual trial.

In conclusion, it must be noted that although video conferencing has been praised and described as a key tool for reducing case backlog in Ugandan courts as it reduces the time spent on hearing the court cases, by the government authorities and different scholars, I argue that caution must be exercised while adopting and replacing physical hearings with virtual hearings due to the underlying effects associated with video conferencing that negatively affect the enjoyment and violate the accused's right to a fair trial as evidenced in this paper.

THE PLACE OF DIGITAL SURVEILLANCE UNDER THE AFRICAN CHARTER ON HUMAN AND PEOPLES' RIGHTS AND THE AFRICAN HUMAN RIGHTS SYSTEM IN THE ERA OF TECHNOLOGY

Mujib Jimoh*

ABSTRACT

All the main international human rights instruments, except the African Charter on Human and Peoples' Rights (the "African Charter"), contain the right to respect for private life, the home and correspondence. This right protects unlawful and unnecessary surveillance. Different theories have been propounded by scholars about the absence of this right in the African Charter. The most prominent and acceptable theory is that the African Charter mirrors African Traditional Values and that under the African system of communalism, privacy is somewhat respected, in contrast with the wide privacy notion under Western liberalism. However, in the era of surveillance technologies where States are able to use these technologies to violate privacy, there is a question about the sustainability of the notion of the "somewhat respect for privacy" in the African human right system. This paper answers this question, and in addition, answers the following: (i) to what extent can and should digital surveillance be permitted under the African human rights system; and (ii) is there any provision in the African Charter that can protect Africans from unnecessary digital surveillance by African States? The paper finds that African States use surveillance technologies for illegitimate purposes, despite the fact that Africa is technologically behind. Therefore, it argues for the formulation of a binding instrument on privacy; a framework for the use of technology in Africa; and the enactment of surveillance laws which are necessary, legitimate, effective and proportional.

* LLB (First Class Hons.), *Ibadan*; BL, *Nigeria Law School*; LLM (Cand.) *Duke University*. Email: mujib.jimoh@duke.edu

INTRODUCTION

Various international human rights instruments contain the right to respect for private life, the home and correspondence.[1] This right protects unlawful and unnecessary surveillance.[2] This right is however, lacking in the African Charter on Human and Peoples' Rights (the "Charter"). Expectedly, some scholars have engaged in debates about the reason for the absence of this right in the Charter.[3] The most dominant view, given the uniqueness of the Charter,[4] is that the privacy contained in other international instruments available at the time of drafting the Charter mirrored Western liberalism – which was thought to be too wide,[5] and too individualistic – that the drafters of the Charter felt it would be incompatible with the African culture and the communitarian ontology to include such right in the Charter.[6] However, this does not mean that privacy was not existent in Africa,[7] but it was *somewhat* recognized within the communal system.

In modern times, it has become imperative to consider the extent to which the *somewhat* recognition of privacy under the African human rights system can be sustained in light of emerging technologies, which affect culture and human

[1] See Universal Declaration of Human Rights (UDHR), art. 12; International Covenant for Civil and Political Rights (ICCPR), art. 17; European Convention on Human Rights (ECHR), art. 8; American Convention on Human Rights (ACHR), art. 11.

[2] Council of Europe, *Impact of the European Convention on Human Rights: Right to Privacy* <https://www.coe.int/en/web/impact-convention-human-rights/right-to-privacy> accessed 6 June 2022.

[3] Two of the scholars who have engaged in a debate about the absence of this right in the African Charter are Professor Alex B. Makulilo and Professor Kinfe M. Yilma. In a forthcoming paper, I tagged this debate the 'Makulilo-Yilma debate'. Yilma believes the absence was "probably a mere drafting oversight'. See Kinfe M. Yilma, 'The Quest for Information Privacy in Africa: A Review Essay' (2017) 7 Journal of Information Policy 111-119. Makulilo believes Africa suffered from 'privacy myopia' before contact with the West and that 'privacy in Africa is principally a Western imported liberal concept'. See Alex B. Makulilo, 'A Person is a Person through Other Persons – A Critic Analysis of Privacy and Culture in Africa' (2016) 7 Beijing Law Review 192-204; Alex B. Makulilo, 'The Quest for Information Privacy in Africa' (2018) 8 Journal of Information Policy 317-337.

[4] For discussion on the uniqueness of the African Charter, see Rose D'sa, 'Human and Peoples' Rights: Distinctive Features of the African Charter' (1985) 29(1) Journal of African Law 72-81; Julia Swanson, 'The Emergence of New Rights in the African Charter' (1991) 12 New York Law School Journal of International & Comparative Law 307-333. Richard Gittleman, 'The African Charter on Human and Peoples' Rights: A Legal Analysis' (1982) 22(4) Virginia Journal of International Law 667-714; Ziyad Motala, 'Human Rights in Africa: A Cultural, Ideological, and Legal Examination' (1989) 12 Hastings International and Comparative Law Review 373-410.

[5] The following quote by William Pitt exhibits the nature of Western privacy: 'The poorest man may in his cottage bid defiance to all the force of the crown. It may frail, its roof may shake, the wind may blow through it; the storms may enter; the rain may enter but the king of England cannot enter; all his forces dare not cross the threshold of the ruined tenement.' See H. Brougham, *Historical Sketches of Statesmen in the Time of George III – to Which Are Added Remarks on the French Revolution (Read Books 2007).*

[6] Akin Ibidapo-Obe, *Essays on Human Rights Law in Africa* (Concept Publications Ltd 2005) 260; Osita Ogbu *Human Rights Law and Practice in Nigeria* (2nd revised edn, Snaap Press Ltd 2013) 280-281. See also Julia Swanson, 'The Emergence of New Rights in the African Charter' (1991) 12 New York Law School Journal of International & Comparative Law 307-333 at 327.

[7] *Yilma* (n3).

rights.[8] One such area to consider is the issue of digital surveillance, and its effect on privacy in Africa. One might be curious to know: is there any provision in the Charter which protects Africans from unnecessary digital surveillance in the era of technology, considering that the right to privacy, which should serve this purpose, is absent in the Charter? One may also ask: to what extent can and should digital surveillance be permitted under the African human rights system? The foregoing is part of the questions this paper answers.

This paper conceptualizes the term 'technology'. As popular as the term is, it is said to be one of the most 'confused'.[9] What is however clear is that etymologically, 'technology' has its roots 'in the Indo-European root *tek*, a term that probably referred to the building of wooden houses by wattling, that is, weaving sticks together'.[10] It is Agar's view that though 'we are probably comfortable with asserting that humans have had technologies since the Paleolithic, and a menagerie of animals, from crows to chimps, have even been identified as tool users, 'technology' is of surprisingly recent vintage.'[11] This paper conceptualizes technology as 'a system created by humans that uses knowledge and organization to produce objects and techniques for the attainment of specific goals'.[12] Notwithstanding that we may be able to trace technology to the Paleolithic from the foregoing definition, this paper limits the scope of technology to modern technology like computers, modern machine, robotics, artificial intelligence and big data.[13] Also, whilst surveillance existed before the advent of technology,[14] this paper conceptualizes it as the use of technologies to monitor, intercept and exploit communication and information.[15]

In addressing the questions raised by this paper, the paper is divided into four parts. After this introduction, part 2 discusses the relationship between technology, individualism and communalism under the African human rights system. Part 3 discusses digital surveillance in Africa and its effects on human rights in the continent. Part 4 discusses the protection of privacy and the place of digital surveillance under the African human rights system and makes some recommendations before drawing the conclusion.

[8] Jennifer M. Myers, 'Human Rights and Development: Using Advanced Technology to Promote Human Rights in Sub-Saharan Africa' (1998) 30(2) Case Western Reserve Journal of International Law 343.
[9] Jon Agar, 'What is Technology' (2020) 77(3) *Annals of Science*, 377-82, 377.
[10] ibid 108.
[11] ibid.
[12] La Shun L. Carroll, 'A Comprehensive Definition of Technology from an Ethological Perspective' (2017) 6 Soc. Sci 126.
[13] Thus, where the term technology is used in this paper, it means the same as modern technology.
[14] For a comprehensive discussion from a South African perspective, see Michael Kwet, 'Surveillance in South Africa: From Skin Branding to Digital Colonialism' in Jeffrey Vagle and Michael Kwet (eds), *The Cambridge Handbook of Race and Surveillance* (forthcoming).
[15] Surveillance and digital surveillance are used interchangeably in this paper. Also, whilst surveillance may be done by private individuals and States, the paper considers it from the perspective of State surveillance.

2. THE STATE OF PRIVACY UNDER THE AFRICAN HUMAN RIGHTS SYSTEM: INDIVIDUALISM, COMMUNALISM AND TECHNOLOGY[16]

The Charter, which is the principal international human rights instrument in Africa, underscores the notion of communalism.[17] Although a school of thought believes that the beginning of Statehood in Africa signalled the end of the communal value of the African society,[18] at the time of clamouring for a human rights instrument in Africa, which also coincided with the clamour for African Statehood,[19] the idea of having a human rights instrument with only individual rights was not conceived. Rather, discussions were on an African human rights instrument which recognized both communal and individual rights. For instance, at the 16th Ordinary Session of the African Union ("AU") in 1979, when the Charter was still being debated,[20] the AU called for the preparation of 'a preliminary draft of an African Charter on Human and *Peoples'* Rights providing for the establishment of organs and for the promotion and protection of human and *peoples'* rights.'[21] Thus, the Charter contains not only 'human' rights',[22] but also 'peoples' rights.[23]

It has been maintained that the idea of including peoples' rights in the Charter underscores the notion that communal rights are greater than individual rights.[24] According to Gittleman, 'the notion of individual responsibility to the community is firmly ingrained in African tradition and is therefore consistent with historical traditions and values of African civilization upon which the Charter relied.'[25] The inclusion of collective or communal rights in the Charter is unique and contrasts with other international human rights instruments, like the European Convention on Human Rights and the American Convention on Human Rights.[26] This notion of communality is deeply integrated in the Charter and it is a core value upon which the Charter rests.[27] Murray and Wheatley state that:

> [T]he values of the African societies differ from those of Western societies, with

[16] For a comprehensive discourse on privacy in Africa, see Alex B. Makulilo, *Privacy and Data Protection in Africa*, (Scholars' Press 2014) 1-572; Alex B. Makulilo (ed), *African Data Privacy Law* (Springer Cham 2016).

[17] Richard Gittleman, 'The African Charter on Human and Peoples' Rights: A Legal Analysis' (1982) 22(4) Virginia Journal of International Law 667-714.

[18] Walter Rodney, *How Europe Underdeveloped Africa* (Bogle-L'Ouverture Publications 1972) at 140; Temitope Fagunwa, 'Ubuntu: Revisiting an Endangered African Philosophy in Quest of a Pan-Africanist Revolutionary Ideology; (2019) 3(45) Genealogy 1-17.

[19] Nii L. Bruce-Wallace, 'Africa and International Law – the Emergence to Statehood' (1985) 23(4) The Journal of Modern African Studies 575-602; Rachel Murray, *Human rights in Africa from the OAU to the African Union*, (Cambridge 2000) 1-267

[20] The Charter entered into force on 21 October 1986. See Frans Viljoen, 'Application of the African Charter on Human and Peoples' Rights by domestic courts in Africa' (1999) 43(1) Journal of African Law 1.

[21] *Gittleman* (n18) 667.

[22] Charter, arts. 1-18.

[23] Charter, arts. 19-24.

[24] *Gittleman* (n18) 673.

[25] ibid.

[26] OHCHR, *Minority Rights under the African Charter on Human and Peoples' Rights* <https://www.ohchr.org/Documents/Publications/GuideMinorities6en.pdf> accessed 15 June 2022

[27] *Gittleman* (n18) 676

> the notion of community central to the African way of life: a person is not regarded as an isolated and abstract individual, but an integral member of a community. In Africa, "man is part and parcel of society." The African Charter on Human and Peoples' Rights (ACHPR) makes clear that the rights of an individual are bound up with and thus only realized with the context of the community in which those rights are not restricted, but rather protected …[28]

Despite many praises for the Charter,[29] it has been criticized for the absence of a privacy provision.[30] There is a view which proposes that the reason of this is because of an indirect proportionality between privacy and communalism. Privacy, according to some scholars, is an individualistic right.[31] The view posits that the reason for the absence of a privacy provision in the Charter is because, privacy being an individualistic right, cannot co-exist in an instrument like the Charter, which ingrains the principle of communalism. This view theorizes that individualism is a condition precedent for privacy to develop.[32] Thus, the view downplays the development of privacy in Africa due to its communal nature. However, this view has been criticized and rejected, rightly, by some scholars. Makulilo opines that:

> An overview of the above scholarship (about privacy and culture in Africa) reveals that the first strand over-emphasises individualism not only as a permanent natural condition but also a pre-condition for privacy to develop. This is misleading …[33]

The view that there is an indirect proportionality between communalism and privacy is fallacious, at least, for one reason. The view seems to suggest that individuals cannot have personal rights in a communitarian setting. But this cannot be correct. Taylor offers an insight when he posits that the choice is not always between a close, family-like community and a modern, impersonal society since it is possible to have a 'communitarian or holist ontology and to value liberalism's individual rights.'[34] Within the communal system of the African society, both individual and collective privacy[35] were/are recognized.[36] Even with technology in

[28] Rachel Murray and Steven Wheatley, 'Groups and the African Charter on Human and Peoples' Rights' (2003) 25(1) Human Rights Quarterly 213, 215.
[29] Abiodun J. Osuntogun, 'An Appraisal of the Rights in the African Charter on Human and Peoples' Rights and Notable Institutions for their Enforcement' (2016) 4(1) Akungba Law Journal 332.
[30] Moussa Samb, 'Fundamental Issues and Practical Challenges of Human Rights in the Context of the African Union' (2009) 15(1) Annual Survey of International & Comparative Law 61-74, 64.
[31] Daniel Solove, *Understanding Privacy*, (Cambridge, MA: Harvard University Press 2008) 39; Agnidipto Tarafdah, 'Surveillances, Privacy and Technology: A Comparative Critique of the Laws of USA and India' (2015) 57(4) Journal of the Indian Law Institute 550-578, 550.
[32] *Makulilo* (2018) (n3) 320.
[33] Ibid.
[34] Charles Taylor, 'Cross-purposes: The Liberal-Communitarian Debate' in Nancy Rosenblum (ed) *Liberalism and the Moral Life* (Harvard University Press 1991) at 161; Charles Taylor, 'Communitarianism, Taylor-made: An interview with Charles Taylor' (1996) 68(2) Australian Quarterly 1-10, 3; Moeketsi Letseka, 'In Defence of Ubuntu' (2012) 31 Studies in Philosophy and Education 47-60, 53.
[35] Collective privacy is the privacy of a group of people. See Woodrow Hartzog, 'What is Privacy? That's the Wrong Question' (2021) 88(7) The University of Chicago Law Review 1677-88.
[36] In a forthcoming paper, I argue, providing evidence of the presence of privacy in Africa using the Yoruba ethic-nation as an example, that privacy existed in Africa before contact with the West. I described a typical Yoruba compound which shows the presence of privacy. See Nathanie Fadipe,

modern times and amidst the concern that it fosters individualism, both individual and collective privacy are recognized and regarded as important.[37]

Notwithstanding the absence of a privacy provision in the Charter, subsequent international instruments and Declarations adopted pursuant to the Charter, even with their limitations,[38] recognize this right. For instance, the African Charter on the Rights and Welfare of the Child[39] provides that 'no child shall be subject to arbitrary or unlawful interference with [one's] privacy, family home or correspondence, or to the attacks upon honour or reputation...'[40] The 2019 African Declaration on Freedom of Expression and Access to Information[41] also states that 'everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information'.[42]

However, one must agree with the view that with the advent of technology, the African communal society is gradually waning[43] and steadily becoming individualistic, culminating in the development of a new sub-set of privacy[44] – data privacy – which underscores the protection of individual's personal information. Roos propounds that the law is always challenged by new technological advancement.[45] On privacy, she opines that three eras of technological inventions culminated in the development of privacy law. The first is the 'new miniature camera technology' which influenced the popular Warren and Brandeis's article,[46] with the concern at the time being that such technology could be used by 'sensationalist press to publish pictures of individuals without their consent'.[47] The second, according to Roos, is the 'introduction of computers in the 1950s' with the concern about the misuse of personal information since computers are able to store

The Sociology of the Yoruba (Ibadan University Press 1970); Olanrewaju. Shitta-Bey, 'The Family as Basis of Social Order: Insights from the Yoruba Traditional Culture' (2014) 23 International Letters of Social and Humanistic Science 79-89.

[37] *Hartzog* (n36) 1684.

[38] The African Charter on the Rights and Welfare of the Child is limited in a way. It protects the African Child defined in Article II as a person below the age of 18. Thus, it is not applicable to all persons. Also, whilst the 2019 African Declaration on Freedom of Expression and Access to Information protects the privacy of 'everyone', the Declaration is not binding under international law. See DAGDOK, *International Law: Conventions and Declarations* <http://dagdok.org/un-by-subject/international-law/conventions-and-declarations/> accessed 20 June 2022.

[39] The African Charter on the Rights and Welfare of the Child is made pursuant to the Charter. See The African Charter on the Rights and Welfare of the Child, Preamble, Clause 2.

[40] The African Charter on the Rights and Welfare of the Child, art. X.

[41] The 2019 African Declaration on Freedom of Expression and Access to Information was adopted by the African Commission on Human and Peoples' Rights pursuant to Article 45 of the Charter which mandates the African Commission to promote human rights in Africa. See The 2019 African Declaration on Freedom of Expression and Access to Information, Preamble, Clause 1.

[42] The 2019 African Declaration on Freedom of Expression and Access to Information, Principle 40.

[43] *Makulilo* (2016) (n17) 10-15; See also Vaunne Ma and Thomas J. Schoeneman, 'Individualism Versus Collectivism: A Comparison of Kenyan and American Self-Concepts' (1997) 19 Basic and Applied Social Psychology 261-273.

[44] See Anneliese Roos 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) 129(2) South African Law Journal 375-402.

[45] ibid 375. See also Lyria Moses, 'Why Have a Theory of Law and Technological Change' (2007) 8(2) Minnesota Journal of Law, Science & Technology 589-606, 594-595.

[46] Louis Brandeis and Samuel Warren, 'The Right to Privacy' (1890) 4(5) Harvard Law Review193-220.

[47] *Roos* (n45) 375.

information;[48] whilst the third is the development of 'private computers and communication networks'.[49] Hence, in Africa, just like in other parts of the world, it became necessary to develop a framework which addresses the introduction of data privacy as an impact of technology on privacy.

So much have been written about the impact of technology on privacy.[50] One area that has been well considered is the emergence of 'data privacy' due to the advent of technology. Though there is a relationship between privacy and data privacy, the advent of technology has necessitated the need for special protection.[51] It is generally agreed that whilst most African countries have privacy provisions in their constitutions,[52] such provisions might not be sufficient to contain the impact of technology and the internet on privacy, hence, the need for data privacy protection. For instance, it is declared in the Supplementary Act on Personal Data Protection within ECOWAS (the Supplementary Act) that 'notwithstanding the existence of the national legislations relating to the protection of privacy of the citizens in their private and professional life and relating to the guarantee of the free movement of information, it becomes a matter of urgency to fill the legal vacuum generated by the use of internet which is a new instrument of communication'.[53]

At the international stage, the AU in 2014 adopted the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) where it is declared that the AU 'aware that it is meant to regulate a particularly evolving technological domain, and with a view to meeting the high expectations of many actors with often divergent interests…'[54] Surprisingly, the Malabo Convention, despite its comprehensiveness in addressing privacy issues in the use of technology in Africa,[55] has not been ratified. Article 36 of the Malabo Convention provides that the Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the AU of the fifteenth (15th) instrument of ratification. Since 2014 when the Malabo Convention was adopted, only fourteen (14) of fifty-five (55) AU member States have signed it and only seven have ratified it.[56] Also, at the domestic stage, the situation is not any better. According to the UNCTAD, only thirty-three (33) of the fifty-four (54)

[48] ibid at 376.
[49] ibid at 377.
[50] See *Hartzog* (n36); Michelle Cayford and Wolter Pieters, 'The Effectiveness of Surveillance Technology: What Intelligence Officials Are Saying '(2018) 34(2) The Information Society 88-103; Glenn Greenwald *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (1st edn Metropolitan Books/Henry Holt, 2014); Eriola Cakrani, 'Technology and Privacy, Internet Effects on Privacy' (2013) 4(9) Mediterranean Journal of Social Sciences 279-283; Hall Berghel, 'Through the PRISM Darkly' (2013) 46(7) Computer 86–90.
[51] See The South African Development Community (SADC) Data Protection Model Law, Preamble, Clause 10.
[52] *Yilma* (n3) 115.
[53] The Supplementary Act on Personal Data Protection within ECOWAS, Preamble, Clause 10.
[54] See The Malabo Convention, Preamble, Clause 8
[55] 'African Countries Urged to Ratify Malabo Convention' (*itweb*, 10 September 2021) <https://itweb.africa/content/GxwQD71ZJy4MlPVo> accessed 30 June 2022; 'Malabo Convention: African Data Regulators Call for Action' (*Unwanted)* <https://www.unwantedwitness.org/malabo-convention-african-data-regulators-call-for-action/> accessed 30 June 2022.
[56] To access the status list, see <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> accessed 16 June 2022.

African States have data protection and privacy legislation.[57] Even in States with the legislation, about half is not yet in force.[58]

There are also some efforts by the African Regional Economic Communities (RECs) to protect data privacy in the era of technology. For instance, in 2010, ECOWAS adopted the Supplementary Act 'conscious…that the increasing use of information and communication technology (ICT) may be prejudicial to the private and professional life of the users'.[59] To make the Supplementary Act binding on member States, it is annexed to and forms an integral part of the ECOWAS Treaty.[60] In fact, the Supplementary Act is the first, and remains the only, international data protection law in Africa that is binding.[61] Though there are also the East African Community Legal Framework for Cyberlaws and the Southern African Development Community (SADC) Data Protection Model Law whose aim is to ensure the harmonization of data protection policies in member States. Despite the foregoing, as a whole, there is no binding African international law protecting privacy right; Africa does not have a framework to address human rights issues in the use of technology[62] and it lacks the framework for the enforcement of data protection.[63] Thus, the state of privacy in Africa is such that needs to keep up with the advent of technology for a continued safeguard of the privacy rights of Africans.

3. THE EFFECTS OF DIGITAL SURVEILLANCE IN AFRICA IN THE ERA OF TECHNOLOGY

The advancement in technology in modern times is directly proportional to the spread of digital surveillance.[64] Hence, it is not surprising that most governments in

[57] These countries are: Angola, Cape Verde, Seychelles, Burkina Faso, Mauritius, Tunisia, Senegal, Benin, Morocco, , Gabon, Lesotho, Ghana, Ivory Coast, Mali, South Africa, Madagascar, Chad, Malawi, Equatorial Guinea, Sao Tome e Principe, Guinea, Mauritania, Niger, Algeria, Botswana, Nigeria, Uganda, Kenya, Republic of Congo, Togo and Egypt, Zimbabwe; see UNCTAD, *Data Protection and Privacy Legislation Worldwide* <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>; Securiti, *Checklist of African Data Protection Law* <https://securiti.ai/wp-content/uploads/2022/01/African-Data-Protection-Laws.pdf> accessed 17 June 2022.

[58] Graham Greenleaf and Bertil Cottier 'Comparing African Data Privacy Laws: International, African and Regional Commitment' (2020) 32 UNSWLRS 1-37.

[59] Supplementary Act, Clause 9

[60] Supplementary Act, art. 48

[61] African Declaration on Internet Rights and Freedoms Coalition, *Privacy and Personal Data Protection in Africa: A Rights-Based Survey of Legislation in Eight Countries* p. 188; Ololade Shyllon, 'The Right to Privacy and the Protection of Personal Information in Africa: Challenges and Prospects' (2017) <https://aanoip.org/wp-content/uploads/2018/07/Privacy-and-Data-Protection-IB-Dec-2017.pdf>

[62] In 2021, the African Commission on Human and Peoples' Rights declared in its 473 Resolution that Africa does not have a huma rights framework for the use of AI, Robotic and emerging technologies. To access the Resolution, please see <https://www.achpr.org/sessions/resolutions?id=504> accessed 27 June 2022.

[63] Olumide Babalola 'Data Protection Legal Regime and Data Governance in Africa: An Overview' (2022) Aercafrica Policy Brief No. DG003 1-7

[64] Tarafdah (n32) 552. For comprehensive discussion, see Jane Duncan 'Taking the Spy Machine South: Communications Surveillance in Sub-Saharan Africa' in Bruce Mutsvairo (eds) *The Palgrave Handbook of Media and Communication Research in Africa* (Palgrave Macmillan, Cham 2018);

the world, including some African States, engage in the act of surveillance.[65] Digital surveillance is the deployment of technology to monitor, intercept or exploit sensitive data, information or communication.[66] The monitoring, interception or exploitation may take different forms: it could be the use of audio or video surveillance technologies; it could be the use of location monitoring technologies; it could be the use of phone monitoring technologies or internet monitoring technologies.[67]

Generally, in Africa, and in other parts of the world, digital surveillance could be aimed at a target, or it could be mass surveillance. A targeted surveillance is aimed at a specific individual or group; whilst mass surveillance involves the general accumulation of information unmethodically.[68] 'The distinction between targeted and mass surveillance is important, says the European Union, 'both from a legal and policy perspective.'[69] This is because whilst target surveillance could pass international human rights test – if it pursues a legitimate objective – for instance, when deployed for the security of the society, mass surveillance cannot.[70] The concern in Africa is that some governments have embarked on the use mass surveillance, and where target surveillance is employed, it is used as a tool of repression – like victimizing the opposition – rather than pursue legitimate objective.[71]

Technological power does not belong to Africa. This is because technology originated outside Africa[72] and the 'ownership and control of the three core pillars of the digital ecosystem: software, hardware, and network connectivity'[73] lies outside the continent. Thus, most surveillance technologies are imported to African States from China, Europe and the United States.[74] However, paradoxically, despite

---

Williem Gravett 'Digital Neocolonialism: The Chinese Surveillance State in Africa' (2022) 30(1) African Journal of International and Comparative Law 39-58; Lewis Herrington, 'The Debatable Land: Spies, Secrets and Persistent Shadows' (2018) 94(3) International Affairs 645-655; Simon Willmetts, 'The CIA and the Invention of Tradition' (2015) 14(2) Journal of Intelligence History 112-128; CIPESA, *2021 State of Internet Freedom in Africa: Effects of State Surveillance on Democratic Participation in Africa*. Report may be accessed at <https://cipesa.org/2021/09/how-state-surveillance-is-stifling-democratic-participation-in-africa-state-of-internet-freedom-in-africa-study-findings/> accessed 17 July 2022.

[65] Ola El-Ashy *et. al,* 'Big Brother in the Middle-East and North Africa: The Expansion of Imported Surveillance Technologies and their Supportive Legislation' (2019) 3 Global Campus Human Rights Journal 229-249.

[66] Ishan Sharma 'A More Responsible Digital Surveillance Future' (2021), Federation of American Scientist 5.

[67] *Ola El-Ashy et al* (n67) 230.

[68] European Union, *Surveillance and Censorship: The Impacts of Technology on Human Rights* (EP/EXPO/B/DROI /FWC/2013-08/Lot8/02) 10-11.

[69] Ibid.

[70] ibid 11.

[71] There are reports of the use of surveillance on opposition in Uganda. See Bulelani Jili 'The Spread of Surveillance Technology in Africa Stirs Security Concerns' <africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/> accessed 29 June 2022.

[72] This paper has already conceptualized technology as modern technology. See *Roos* (n45); see *Makulio* (2018) (n3) 322-23; Lee Bygrave *Data Privacy Law: An International Perspective* (Oxford University Press 2014) 106; Graham Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press 2014).

[73] *Kwet* (n15) 12.

[74] Tony Roberts (ed) 'Surveillance Law in Africa: A Review of Six Countries' (Brighton: Institute of

the fact that technologically, Africa is lagging behind, somehow, sophisticated digital surveillance technologies are being used by repressive African governments.[75] Human rights reports, articles and research works have shown evidence of the use of surveillance technologies in Algeria, Botswana, Cameroon, Côte d'Ivoire, Egypt, Ethiopia, Equatoria Guinea, Ghana, Libya, Malawi, Morocco, Nigeria, Rwanda, South Africa, Tanzania, Uganda, Zambia and Zimbabwe.[76] Reports show the use of a Deep Packet Inspection technology known as Eagle, which was developed by Amesys, a French company, and deployed by the Libyan government for both target and mass surveillances, where the government was able to 'listen to the entire country'[77] and monitor target individuals.[78] Uganda is also reported to have purchased closed-circuit television camera (CCTV) from Huawei, a Chinese company, for surveillance.[79] There are also reports that a surveillance technology called FinSpy, developed by Gamma International, a company headquarters in Italy, is being used by the Ethiopian government as a tool of mass surveillance.[80] In addition to this, concern has been raised on Ethiopia's Telecom Fraud Offence Proclamation which criminalizes the manufacture, assembly or import of any telecommunications equipment without a permit, and empowers the State to monitor encryption, with its antecedent propensity for surveillance.[81] This concern about monitoring encryption has also been raised in Chad, Malawi, Senegal, Tanzania, Tunisia and Zambia,[82] with stringent punitive laws made as consequences for failure to comply with the laws.[83]

International law generally permits limitations on human rights in certain circumstances.[84] Thus, surveillance laws may be enacted to protect public interest such as national security, public health, morality or the right of others, and there is nothing wrong under the African human rights system, as the African Commission made clear in *Media Rights Agenda v. Nigeria*,[85] with enacting laws to protect these interests. For instance, the *2015 African Guideline on Countering Terrorism* provides that States may interference with privacy if it is necessary to pursue a legitimate (communal) interest.[86] Nevertheless, the concept of 'necessity' is vague,

---

Development Studies, 2021) 8; Jane Duncan, *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa*, (Wits University Press 2018) 1-156.

[75] *Ola El-Ashy et al* (n67) 230.

[76] ibid; *European Union* (n70); *Jili* (n73); *CIPESA* (n64).

[77] *Ola El-Ashy et al* (n67) 231.

[78] See Mark B. Taylor *War Economies and International Law* (Cambridge University Press 2021) 269.

[79] *Jili* (n73) 2.

[80] *European Union* (n70) 11.

[81] Gabriella Razzano *Human Rights and Information in Africa: A Reflection on Trends* (fesmedia Africa, Friedrich-Ebert-Stiftung 2016) 15.

[82] '2021 State of Internet Freedom in Africa: Effects of State Surveillance on Democratic Participation in Africa' (*AfricaPortal* 28 September 2021) <https://www.africaportal.org/publications/state-internet-freedom-africa-2021-effects-state-surveillance-democratic-participation-africa/> accessed 3 July 2022

[83] *CIPESA* (n64) 7.

[84] UNODC, *Limitations Permitted by Human Rights Law* <https://www.unodc.org/e4j/en/terrorism/module-7/key-issues/limitations-permitted-by-human-rights-law.html> accessed 4 July 2022.

[85] *Media Rights Agenda v. Nigeria* (2000) AHRLR 200. See Charter, art. 27.

[86] See Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa, Part 11. As discussed above, the Charter underscores communal rights. See Arts. 19-24. So,

and is susceptible to abuse. Therefore, there is the danger of apparent conflict of surveillance with human rights when deployed for illegitimate purposes.[87] The danger manifests most in a continent like Africa, which has been described as 'an egregious human rights violator'[88] with little respect for human rights.[89] Thus, with technological tools for digital surveillance available to African governments, there is a latent,[90] and there are indeed, more violations of human rights in Africa. Potentially, surveillance can inhibit all human rights and may be used to achieve nefarious objectives.[91] But, this paper discusses its effect on the right to privacy and dignity and freedom of democratic participation in Africa.

Privacy is the most affected human right by digital surveillance. When Miller asserted that, 'it would be a good thing if privacy could be protected, but the war and way of technology and the needs of security have *de facto* made the right to privacy a dead letter,'[92] he was probably referring to digital surveillance. There are many reports documenting the impacts of digital surveillance on privacy. The International Federation for Human Rights (FIDH) has released some of these reports; has been a major advocate against the use of surveillance to erode privacy right in Africa; and has even sued some technology companies that develop digital surveillance technologies which have been used illegitimately in Africa.[93] Also, a group of researchers reviewed the law and surveillance in six (6) African countries and concluded that these States, through their surveillance, violate the right to privacy; and that no one has been prosecuted for it.[94] Writing about how surveillance affects privacy in Africa, Jili states that:

Remote-control hacking is another form of surveillance technology that is spreading across the continent. These surveillance systems enable governments to access files on targeted laptops. They also log keystrokes and passwords as a means to turn on webcams and microphones. Eavesdropping is another surveillance technique that allows governments to access calls, texts, and the locations of phones around the world. This technique, most closely linked to the Bulgarian-based surveillance firm Circles, an affiliate of the NSO Group, which developed the infamous Pegasus software, provides spyware technology to countries as a means to exploit faults in telecom systems. Several governments in African countries, such as Botswana, Equatorial Guinea, Kenya, Morocco, Nigeria,

---

it is not surprising that the Guideline contains such provision.

[87] *CIPESA* (n64) 16.

[88] Makau Mutua, 'The African Human Rights Court: A Two-Legged Stool?' (1999) 21 Human Rights Quarterly 342.

[89] Manisuli Ssenyonjo 'Responding to Human Rights Violations in Africa: Assessing the Role of the African Commission and Court on Human and Peoples' Rights (1987–2018)' (2018) 7 International Human Rights Review 1.

[90] *Gravett* (n65) 39.

[91] The use of technology for political, economic, and social domination has been well documented in various reports. See for instance *Jili* (n73); *Ola El-Ashy et al* (n67).

[92] Jeremy M. Miller, 'Dignity as a New Framework, Replacing the Right to Privacy' (2007) 30(1) Thomas Jefferson Law Review 1-52, 1.

[93] For instance, FIDH sued Amesys in a French court. See FIDH Submission to the *UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: The Surveillance Industry and Human Rights* < https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/FIDH.pdf> accessed 5 July 2022.

[94] The six countries are Egypt, Kenya, Nigeria, Senegal, South Africa and Sudan. See *Robert (ed)* (n76).

Zambia, and Zimbabwe, are reportedly using these systems to connect to their local telecommunications companies' infrastructure to conduct surveillance.[95]

The concern about the impact of surveillance on privacy is further compounded by lack of a framework in Africa to address this, most of the which have been discussed earlier in this paper. First the Charter, which is the principal international human rights instrument in Africa, does not contain a privacy provision.[96] Secondly, there is no binding international instrument for data protection in Africa, other than the Supplementary Act, which is only binding on ECOWAS States.[97] Thirdly, whilst there are other instruments and Declarations which contain privacy provisions in Africa, there are limitations to them. The African Charter on the Rights and Welfare of the Child, though has a privacy provision, is applicable to a child – person under the age of 18,[98] and Declarations – such as the 2019 African Declaration on Freedom of Expression and Access to Information – are generally not binding under international law. There is thus a *lacuna* to address.

Surveillance may also aid in the violation of, and interference with, the right to dignity.[99] Dignity is a *jus cogens*, for which no derogation is permitted.[100] The right to dignity is protected and contained in all major international instruments,[101] including the Charter[102] and constitutions of African States.[103] There are scholars who believe that privacy is inherent in the right to dignity, such that the right to dignity of an individual may be violated if their privacy is infringed.[104] Roos, a leading scholar on privacy in Africa, disagrees however, stating that this is 'confusion'. 'If it is kept in mind that privacy as a personality interest is only infringed when someone learns of true private facts about a person against the person's will', states Roos, 'the difference between privacy and other personality objects [like dignity] becomes clear.'[105] Nonetheless, without necessarily waging

[95] *Jili* (n73) 2.

[96] This is not to say there is/was no privacy in Africa. The only concern here is how to proceed in enforcing a right not contained in the Charter before the African Court on Human and Peoples' Rights and the African Commission on Human and Peoples' Rights if domestic remedy cannot be obtained. See Sabelo Gumedze 'Bringing Communications before the African Commission on Human and Peoples' Rights' (2003) 3 African Human Rights Law Journal 118-148.

[97] These States are Benin, Burkina Faso, Cabo Verde, Cote d'Ivoire, The Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo.

[98] The African Charter on the Rights and Welfare of the Child, art. II

[99] *CIPESA* (n64) 29.

[100] James Rachels, 'Kantian Theory: The Idea of Human Dignity' (1986) <https://public.callutheran.edu/~chenxi/phil345_022.pdf> accessed 13 July 2022.

[101] UDHR, art. 1; ICCPR, art. 10. Although not expressly provided in the ECHR, the jurisprudence of the European Court confirms that dignity is a recognized right. See Sebastian Heselhaus and Ralph Hemsley 'Human Dignity and the European Convention on Human Rights' in Paolo Becchi and Klaus Mathis (eds) *Handbook of Human Dignity in Europe* (Springer Cham 2019).

[102] Charter, art. 5

[103] See for instance 1999 Constitution of Nigeria, s. 34; South Africa Constitution, s.12.

[104] Avani Singh and Michael Power, 'The Privacy Awakening: The Urgent Need to Harmonise the Right to Privacy in Africa' (2019) 3 African Human Rights Yearbook 202-220; Kinfe M. Yilma and A. Birhanu, 'Safeguards of the Right to Privacy in Ethiopia: A Critique of Laws and Practices' (2012) 26 Journal of Ethiopian Law 109-110.; *Robert* (n76) 180. See also Justice Alfred Mavedzenge, 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework which Guarantees Proportionality in Communications Surveillance' (2020) 12(3) African Journal of Legal Studies 360-390.

[105] Anneliese Roos, 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study' (PhD thesis, University of South of Africa, 2003) 557.

into this debate, there are reports of the use of surveillance to aid the violation of dignity of persons in Cameroon, Kenya, Mozambique, Nigeria, Tanzania and Uganda after violating their privacy.[106] The UN Special Rapporteur observed that 'there are credible indications to suggest that digital technologies have been used to gather information that has then led to torture and other ill-treatment.'[107] Some of the victims' accounts go thus:

> [1]: I do not really know how they do it … because when they arrested me I found them with my voice calls I had with my interviewees in the story I had published. That made me sure that they had intercepted my communications.
>
> [2]: I learnt that security agencies were listening to my calls when people I used to call would be arrested the following day. While being tortured, the recordings of our conversations would be played or sometimes they were told what I said when talking to them.[108]

The use of surveillance to suppress the freedom of democratic participation in Africa is also well documented. CIPESA released a report in 2021 on the effects of state surveillance on democratic participation in Africa.[109] Article 13 of the Charter guarantees the democratic right to participate freely in government. Sadly, African States have used surveillance to target opposition leader and civil societies. For instance, it has been found that intelligence officials in Uganda used surveillance technology to crack the encrypted communications of opposition leader, Bobi Wine.[110] This has also been discovered in some other African States.[111]

Notwithstanding the foregoing, when deployed for legitimate purposes, surveillance may avert potential dangers to the society. Cayford and Pieters are amongst the scholars who have documented some of the positive uses of surveillance technologies. In their article,[112] they document how the United Kingdom intelligence agencies have depended on 'the fantastic work that GCHQ do to detect terrorist communications. That leads to us finding terrorist plots that we would not otherwise find, that we are then able to thwart, which leads to lives being saved'[113] They also note how drones, equipped with missiles, 'have not only disrupted terrorist plots, but it also reduced the original Qaeda organization along the Afghanistan Pakistan border to a shell of its former self".[114] In light of these positive uses of surveillance technologies, therefore, the issue to address in Africa is how to ensure that surveillance technologies are used to pursue and achieve legitimate purposes only.

Data protection laws originated from North America and Europe. Greenleaf notes that 'data privacy laws originated as a "Western" notion, in that their earliest legislative instantiations were in North America (1970 and 1974), and in seven western

---

[106] *CIPESA* (n64) 5.
[107] See 'The Right to Privacy in the Digital Age' A/HRC/27/37 (2014) para 14.
[108] *CIPESA* (n64) 17.
[109] ibid
[110] *Jili* (n73) 1.
[111] *Robert* (n76) 4.
[112] *Cayford and Wolter Pieters* (n51).
[113] ibid 93.
[114] Ibid.

European countries in the 1970s."[115] He further notes that 'the principal players who negotiated their transformation into an international standard, the OECD Guidelines, in 1978–80 were from Europe, North America, and Australasia.'[116] Europe is the leading continent to emulate in the realm of data protection. Because the United State does not have a single data protection law,[117] but rather different data protection laws for different specific data,[118] there is a clamour for the government to develop a national privacy policies and standards in order to balance the privacy right of citizens against surveillance and national security.[119] The general rule in the United States is that surveillance is permitted, except in certain circumstances.[120] Whilst the Fourth Amendment to the United States Constitution protects some form of privacy right,[121] the United States Supreme Courts has not strictly upheld privacy right when there is a compelling State's interest.[122] In the wake of the 9/11 incident, the United Sates has put in surveillance measures, which privacy and data privacy advocates have criticized, to promote its national security. According to Richards:

Government investigators in antiterrorism cases possess a powerful tool known as the National Security Letter (NSL). NSLs are statutory authorizations by which the FBI can obtain information about people from their telephone companies, Internet service providers, banks, credit agencies, and other institutions with which those people have a relationship. NSLs are covert and come with a gag order that prohibits the recipient of the letter from disclosing its existence, even to the person whose secrets have been told to the government. NSLs can currently be obtained under four federal statutes: the Right to Financial Privacy Act of 197842 (RFPA), the ECPA,43 the Fair Credit Reporting Act44 (FCRA), and the National Security Act of 1947.[123]

Due to more emphasis on national security, scholars believe that the current data protection laws in the United States have not been effectual in striking a balance between individual privacy right and national security.[124] Whereas in Europe, there is a rich legal regime for data protection.[125] The first law on data protection was made in Europe (Germany) in 1970 in response to some surveillance activities.[126] In 2018, the General Data Protection Regulation (GDPR), Europe's most popular

[115] *Greenleaf* (n73) 11.
[116] Ibid.
[117] Robert Hasty, Trevor W. Nagel and Mariam Subjally *Data Protection Law in the USA* (Advocates for International Development 2013) 1-28.
[118] See for instance the Privacy Act of 1974; Health Insurance Portability and Accountability Act of 1996; USA PATRIOT Act, 2001; The Family Educational Rights and Privacy Act. See Stephen Cobb 'Data Privacy and Data Protection' (2016) ESET White Paper 1-15, 3 and Michael Walter-Echols, 'Panopticon – Surveillance and Privacy in the Internet Age' (BSC project, Worcester Polytechnic Institute, 2009) 13-14.
[119] John Shattuck and Mathias Risse 'Reimagining Rights & Responsibilities in the United States: Privacy, Personal Data, and Surveillance' (2021) 016 Carr Center for Human Rights Policy 25
[120] Neil Richards 'The Danger of Surveillance' (2013) 126 Harvard Law Review 1934.
[121] The text of the Fourth Amendment does is not worded in absolute terms but those deemed unreasonable.
[122] *Walter-Echols* (n119) 10.
[123] *Richards* (n121) 1492.
[124] *Cobb* (n119) 10.
[125] For a brief history of data protection in Europe, see Hendrik Mildebrath *Understanding EU Data Protection Policy* (European Parliamentary Research Service 2022).
[126] Ibid 2

data protection legal instrument, entered into force. Although the GDPR gives European Union (EU) States the discretion in balancing data privacy right and national security,[127] such measures taken by the State should be "necessary and proportionate".[128] The GDPR is a comprehensive legal instrument on data protection in Europe. For instance, it contains provisions on 'adequacy decision'.[129] The adequacy decision allows the transfer of data from the EU to a third country if it is shown that the third country has data protection standard similar to the EU standards. In the recent *Schrems cases,* the Court of Justice of the European Union (CJEU) held that the EU's arrangement with the United States to transfer personal data to the United States was illegal due to the surveillance policy in the United States.[130] In effect, the *Schrems cases* validated the view that the United States has a lesser protection for data privacy and more legal basis for State surveillance than the EU. Africa may thus find the EU regime on data protection, surveillance and national security more human rights complaint than that of the United Sates.

4. THE PROTECTION OF PRIVACY AND THE PLACE OF DIGITAL SURVEILLANCE UNDER THE AFRICAN HUMAN RIGHTS SYSTEM

One curious question that comes to mind is the extent to which digital surveillance may be permitted under the African human rights system, given some of its positive uses. As stated earlier, the Charter deeply ingrains the notion of communality, where the society is considered to be superior to the individual. Gittleman posits that 'the term "peoples' rights" was included at the insistence of the socialist States, the most vocal of which were Ethiopia and Mozambique. They maintained that the individual had no greater rights than that of the society as a whole.'[131] Articles 19–24 of the Charter contains provisions on 'peoples' rights.' The Charter also includes three (3) articles which stipulate the duties of the individual to the community.[132] Gittleman did excellent job narrating why the Charter includes both collective rights and individual's duty to the community. It is best to hear from him directly:

'The notion of individual responsibility to the community is firmly ingrained in African tradition and is therefore consistent with historical traditions and values of African civilization upon which the Charter relied. The inclusion of this far-reaching clause has roots, however, in factors other than mere tradition and to a large extent explains the various tensions throughout the Charter. The socialist States such as Mozambique and Ethiopia had a difficult time reconciling traditional human rights conventions with socialist philosophy. The notion of "individual" in a socialist State differs markedly from the notion in a capitalist State. As a result, to ensure the eventual adoption of the Charter by all States, the drafters in Dakar stated that if the individual is to have rights "recognized" by the State, he also must have obligations flowing back to the State. The drafters believed that references in

[127] See Treaty of the European Union, art 4(2); GDPR, Preamble, Para 6
[128] Charter of the Fundamental Rights of the European Union, art 52(1); GDPR, art 23.
[129] GDPR, art. 45.
[130] Hendrik Mildebrath *The CJEU Judgment in the Schrems II Case* (European Parliamentary Research Service 2020).
[131] *Gittleman* (n18) 673
[132] Charter, arts. 27, 28 and 29

extant international instruments to an individual's obligations were so vague as to be meaningless. For this reason, the African Charter attempts to rectify this concern by enumerating those obligations imposed upon the individual'[133]

Consequently, it may be argued that where the right of the society will be jeopardized as a result of an action/inaction of an individual, which may only be averted by surveillance, surveillance should be permitted. For instance, insecurity is currently rife in Africa, with the United States Institute of Peace declaring that 'terrorism and extreme violent are arguably Africa's greatest threat in 2021'.[134] There are scholars who believe that in a situation where the security of the society is threatened, surveillance is *necessary* and *justified* in this circumstance.[135] In other words, whilst surveillance may actually prevent a threat to the society, but it must always be used to pursue this legitimate objective.

There are scholars who have further argued that in addition to pursuing a legitimate objective, the surveillance must be *effective* in achieving the legitimate objective: otherwise, it would be pointless and a means to violate individual rights if there is nothing to show for such surveillance.[136] Under the African human rights system, threat to the society/others is the only legitimate objective for which the right of an individual may be suppressed, and thus, for which surveillance may be permitted.[137] At the same time, it is important to lay down a guideline for this so as not use surveillance pursue an illegitimate objective – like repression – and erode individual rights under the pretence of societal rights. D'sa was one of the scholars who identified the potential danger, where States may violate individual rights under the pretence of pursuing a legitimate purpose.[138] Consequently, whilst there are some African States that have enacted laws permitting the governments to conduct surveillance,[139] it is imperative to always consider the justiciability, necessity, legitimacy, effectiveness and proportionality of these laws.[140]

One of the steps in the series of steps to be taken in maintaining a balance and ensuring that surveillance technologies are used for legitimate purpose in Africa, is to, first, have a binding international instrument protecting privacy in Africa. Some scholars have argued that privacy should be imported to, and regarded as, part of the right to dignity contained in the Charter,[141] this has not been tested by both the African Commission and the African Court on Human and Peoples' Rights (the "African Court"). Thus, though African States have privacy provisions in their constitutions, it may be essential that there is an African international instrument safeguarding the privacy of Africans for which Africans may seek to enforce at the African Commission or African Court where domestic remedy cannot be obtained.

---

[133] *Gittleman* (n18) 677

[134] 'Security Challenges in Africa: 2021 and Beyond' (*United States Institute of Peace* 24 February 2021) <https://www.usip.org/events/security-challenges-africa-2021-and-beyond> accessed 17 July 2022.

[135] *Mavedzenge* (n106) 2.

[136] *Cayford and Wolter Pieters* (n51).

[137] Charter, art. 27.

[138] Rose D'sa 'Human and Peoples' Rights: Distinctive Features of the African Charter' (1985) 29(1) Journal of African Law 72-81.

[139] *Mavedzenge* (n106) 2.

[140] *ibid; Cayford and Wolter Pieters* (n51).

[141] Avani Singh and Michael Power 'The Privacy Awakening: The Urgent Need to Harmonise the Right to Privacy in Africa' (2019) 3 African Human Rights Yearbook 202-220

This is because even with rights expressively provided in the Charter, States are using domestic laws to 'claw-back' these rights.[142] In *Article 19 v. Eritrea,*[143] rejecting Eritrea's argument that it could limit the right to freedom of expression under its domestic law, the African Commission held that:

> [If] 'law' is interpreted to mean any domestic law regardless of its effect, States Parties to the Charter would be able to negate the rights conferred upon individuals by the Charter. However, the Commission's jurisprudence has interpreted the so-called claw-back clauses as constituting a reference to international law, meaning that only restrictions on rights which are consistent with the Charter and with States Parties' international obligations should be enacted by the relevant national authorities. The lawfulness of Eritrea's actions must therefore be considered against the Charter and other norms of international law, rather than by reference to its own domestic laws alone.[144]

Secondly, there is need to develop a comprehensive framework for the use of technology in Africa. Such framework will, among others, set the guiding principles for surveillance, and provide adequate checks to prevent abuse by the authorized agencies. In 2021, the African Commission 'noting with concern that the development and uses of AI technologies, robotics and new and emerging technologies have far-reaching consequences on human rights in general, including privacy',[145] calls on 'State Parties to work towards a comprehensive legal and ethical governance framework for AI technologies, robotics and ither new and emerging technologies so as to ensure compliance with the African Charter and other regional treaties.'[146] One of the first steps to achieving this is by undertaking further studies to understand the impacts of technology on human rights. Another step will be for African States to adopt and ratify conventions on technology, for instance, the Malabo Convention, for data protection.

Further, African States should enact laws on surveillance. The laws should contain provisions on the necessity, legitimacy, effectiveness and proportionality of surveillance. The laws should pursue a legitimate objective – for instance, to prevent danger to the society. Whilst it is recognized that laws are not enough[147] as it could be used for an illegitimate purpose, adequate mechanism for seeking remedies in the event that surveillance is used for an illegitimate purpose should be provided.

CONCLUSION

This paper has considered the state of privacy in Africa in the light of surveillance technology. It found that there is lack of a binding international instrument or law on privacy in Africa. It discusses the need for a binding international instrument on privacy in Africa and how technology is gradually

[142] For some discussion on claw-back clauses, see *Gittleman* (n18).
[143] Communication 275/03 – *Article 19 v. Eritrea*.
[144] ibid paras [91, 92].
[145] African Commission on Human and Peoples' Rights Resolution 473, Preamble, Clause 10
[146] *Ibid*, Clause 4.
[147] *Robert (ed)* (n76) 5.

waning the communal tenet of the Charter. It also considers the effects of surveillance technology in Africa and its potential for human rights violations when used for illegitimate purpose. In fact, it found the deployment of surveillance technology as a tool for repression, violation of privacy right and dignity in Africa, despite the fact that Africa is behind technologically. The paper found some positive uses of surveillance technologies and recommends ways to deploy surveillance technology in a human rights compliant manner.

DIGITALISATION AS A POST-COVID-19 ECONOMIC RECOVERY TOOL FOR THE EAST AFRICAN COMMUNITY

Augustine Ochieng[*]

ABSTRACT

This article argues that while digitalization presents opportunities for economic growth and recovery in the East African Community post-COVID-19, it is currently skewed in favour of non-resident online companies at the expense of EAC member states and local digital businesses. The inadequate regional legal framework has failed to adequately regulate non-resident online entities operating in EAC member states, leading to issues like tax evasion, avoidance of regulatory compliance, stifled growth of local startups, and compromised consumer protection. The article proposes the creation of a single digital market in the EAC to leverage the region's population as a whole to compel compliance and maximize the benefits of digitalization. A regional approach that includes laws requiring non-resident online entities to register in an EAC member state to access the regional market, supported by regional competition regulation, can help optimize digitalization's potential while mitigating associated risks.

[*] Advocate of the High Court and East African Community Law Expert.

INTRODUCTION

The COVID-19 pandemic found emerged when the East African Community (EAC) had already signed a Protocol Establishing the East African Community Common Market.[1] Numerous steps had been taken to implement the free movement of people and goods, including tremendous progress in the harmonization of national laws,[2] as well as elimination of Tariff and Non-Tariff barriers.[3] Given the degree of regional co-operation and inter dependence, it was evident that none of the Partner States would be able to counter the pandemic on their own. Subsequently a summit was held on the 12th of May 2020.[4] However, no coordinated regional approach was ever concluded by the Partner States, and many worked independently to counter the virus with differing strategies and varying degrees of success.[5] This was not a challenge associated with the EAC alone as a Regional Economic Community (REC). Even the European Union (EU) had a challenge convincing its member States to come up with a single coordinated strategy.[6] Such was the nature of the COVID-19 pandemic that countering it stringently often carried with it dire economic consequences.[7]

Many of the EAC Partner States were economically fragile, running deficit budgets and heavily dependent on tax revenue to meet their budget requirements.[8] They needed to pool resources to counter the pandemic effectively, but this was never done.[9] The EAC Partner States failed to utilize their integration efforts to shelter their economies. The lesson that is evident from the COVID-19 pandemic was that regional coordination was necessary to effectively counter the pandemic it and its effects. In Uganda, the earlier success the country recorded in fighting the COVID-19 pandemic was nullified because it is still spreading from the

[1]The Protocol on the Establishment of the East African Community Common Market, 2005 was signed in 2010. See also James Thuo Gathi, *African Regional Trade Agreements as Legal Regimes*, (Cambridge University Press, 2011) Pg.190-193.

[2] EAC, 'Study on the Establishment of an East African Community Common Market' (August 2007) Final Report M.A. Consulting Group

[3] Leonard Obura Aloo 'Free Movement of Goods in the EAC' In Emmanuel Ugirashebuja (eds), *East African Community Law Institutional, Substantive and Comparative EU Aspects* (Brill 2017) Pg. 303-310.

[4] Heads Of State Consultative Meeting Of The East African Community Communiqué accessed from https://www.eac.int/communique/1725-communiqu%C3%A9-heads-of-state-consultative-meeting-of-the-east-african-community on the 29th of July 2021

[5] UNDP, 'Socio-economic impact of COVID-19 in Uganda: Short-, Medium-, and Long-Term Impacts on Poverty and SDG's using scenario analysis and system dynamics modeling' (April 2020) Policy Brief by UNDP- Uganda Pg.2-4.
See also Ochieng Augustine, 'Pandemic Exposes Fissures in East Africa's Integration Process' *East African Lawyer* (Silver Jubilee Edition 2020) Pg. 37- 40.

[6]Katya Adler, 'EU closes ranks over COVID-19 surge and vaccine delays' *BBC News* (13th March 2021) accessed from https://www.bbc.com/news/world-europe-56361840 on the 20th June 2021.

[7] United Nations Economic Commission for Africa, 'Economic and Social Impacts of COVID-19 in Eastern Africa 2020' (October 2020), Pg 4-10 < https://www.uneca.org/sites/default/files/SROs/Eastern-Africa/ICSOE-24/edited-srp_english_COVID-19_abridged_version.pdf> accessed on the 202th of June 2022. See also Richard Baldwin and Beatrice Weder di Mauro (eds), 'Economics in the Time of COVID-19' (Centre for Economic Policy Research, 2020)

[8] AfDB, 'East Africa Economic Outlook 2019: Macroeconomic Developments and prospects Political economy of regional integration' (2019), Pg.8-13.

[9] Ochieng Augustine, *Ibid* Pg. 37- 40.

neighbouring countries, and Uganda subsequently underwent a second wave.[10]

As a result of the lack of regional response an sufficient coordination, each of the EAC Partner States was fully exposed to the full economic impact of the COVID-19 pandemic which drastically reduced the tax income of the Partner States.[11] The Partners States had to borrow heavily first to counter the pandemic and later to deal with the shortfalls in tax occasioned by measures to prevent the spread of COVID-19.[12] Even Tanzania that never implemented a full lock down borrowed money to fight the pandemic.[13] The EAC Partner States are currently heavily indebted and need to find means of boosting their local revenue to ensure that further lending does not undermine their economies.[14]

2. ROLE OF DIGITALIZATION IN ECONOMIC RECOVERY

In the midst of the COVID-19 pandemic digitalization emerged as a solution. As lockdowns and travel restrictions were being implemented to prevent the spread of COVID-19, many businesses resorted to online marketing and transactions to access customers. As a result, e-commerce and online transactions thrived during the outbreak of COVID-19. The number of consumers shopping online in Kenya and Tanzania rose by 79% and 72 % respectively following the outbreak of COVID-19.[15] According to the Central Bank of Kenya, following the lock down measures, the volume of mobile money transactions rose by 5,457 worth 564.48 million Kenyan Shillings per day.[16] The total volume of E-commerce within the continent is also reported to have risen after the outbreak of COVID-19.[17] This indicates that digitalization has an critical role in the post-COVID-19 economic recovery of the East African Region. The Partner States have to find ways of leveraging on digitalization for it to work in the best interests of the region.

The current digital platform for digitalization in the East African region was attributed largely to the mobile money revolution in 2007.[18] Mobile money has

[10] Kizzi Asala and Africanews with AP 'Ugandan hospitals under pressure amid COVID-19 pandemic second wave' *Africanews* (10th June 2021) accessed from https://www.africanews.com/2021/06/10/ugandan-hospitals-under-pressure-amid-COVID-19-pandemic-second-wave// on the 20th of June 2022.

[11] United Nations Economic Commission for Africa, 'Economic and Social Impacts of COVID-19 in Eastern Africa 2020' (October 2020), Pg. 4-10.

[12] Berna Namata, 'Spectre of debt defaults haunts EA as COVID-19 shrinks exports, taxes' *The East African,* (05 January 2021) accessed from https://www.theeastafrican.co.ke/tea/business/spectre-of-debt-defaults-haunts-east-africa-3212374 on the 20th June 2022.

[13] *Ibid*.

[14] David Whitehouse**,** 'AfDB says COVID-19 is giving East Africa chance to renegotiate debt' *The Africa Report* (26 April 2021) accessed from https://www.theafricareport.com/82936/afdb-says-COVID-19-is-giving-east-africa-chance-to-renegotiate-debt/ on the 20th June 2021.

[15] UNCTAD, 'Ugandan e-commerce platforms power recovery from COVID-19 crisis' *UNCTAD News* (28th June 2020) accessed from https://unctad.org/news/ugandan-e-commerce-platforms-power-recovery-COVID-19-crisis on the 20th June 2022.

[16] Mariam Saleh, 'Increase in e-commerce due to COVID-19 in Africa 2021, by country' (29th June 2022) accessed from https://www.statista.com/statistics/1233745/share-of-consumers-shopping-more-online-due-to-COVID-19-in-selected-african-countries/ on the 20th of June 2022

[17] UNCTAD 'COVID-19 And E-Commerce: Impact On Businesses And Policy Responses' (2020), Pg.5-10, Pg.9-14 accessed from https://unctad.org/webflyer/COVID-19-and-e-commerce-impact-businesses-and-policy-responses on the 20th of June 2022.

[18] World Bank Group, 'A Single Digital Market for East Africa: Presenting A Vision, Strategic

been credited for enabling many entrepreneurship activities.[19] It's use has become so common that governments have started incorporating mobile payment on their websites.[20] In Tanzania, government taxes and fines can be paid using mobile money.[21] Mobile money also grossly improved financial inclusion, and in an online setting gave producers of items and service providers access to a wider consumer base.[22] Mobile money is just one aspect of technology that is dependent on digitalization and its impact on the regional economy has been tremendous.

With mobile money widely being circulated and used, the pandemic found that the market within the EAC had the capacity to readily transition to electronic transactions.[23] It is difficult to imagine how the region would have fared during the pandemic without mobile money as an alternative reliable medium of payment. The economic impact of the pandemic would more likely have been worse. Mobile Money and other existing online market platforms like Jumia are what enabled business to be conducted even under stringent lockdown that was needed to counter the spread of COVID-19.[24] A large number of companies, including banks have included mobile money platforms as a means of transacting and transferring money. This serves to show how critical digitalization has been in sustaining the economies of the East African Communities during the pandemic.

The success and resilience of mobile money transactions during the pandemic indicates that digitalization has a bigger role to play in the post-COVID-19 economic recovery within the East African region. Digital innovations that emerged during the pandemic are already irreversibly transforming service delivery within the East African region, in Uganda and Kenya the judiciaries have digitalized their case filing systems and boosted their capacity for remote hearing of cases.[25] It is anticipated that such measures will reduce the delays in the filing and hearing of cases. In Rwanda robots and drones were used to test and treat COVID-19 in a bid to protect health workers from exposure.[26] The East African region has had outbreaks of infectious diseases like Ebola. The use of drones and robots in treating infectious diseases could help in the fight of such diseases by reducing the exposure of health workers.

The potential of digitalization in transforming the economies of the East African Partner States is very evident. The duty EAC Partner states have is to create a legal and regulatory climate to ensure the growth of digital platforms in a sustainable manner. In Southeast Asia, having witnessed the potential of particularly E-

---

Framework, Implementation Roadmap, And Impact Assessment' (2018) Pg.27.

[19] Ibid.

[20] OECD, 'Digitalisation and jobs in Africa under COVID-19 and beyond' in OECD**,** *Africa's Development Dynamics 2021: Digital Transformation for Quality Jobs***,** (2021), Pg.41-42.

[21] Ibid

[22] World Bank Group, *Ibid*, Pg.76.

[23] OECD, *Ibid*, Pg.1-12.

[24] UNCTAD 'COVID-19 And E-Commerce: Impact on Businesses and Policy Responses' (2020), Pg.5-10.

[25] The Judiciary, 'Judiciary Launches ECCMIS' *The Judiciary* (02 March 2022) accessed from http://judiciary.go.ug/data/news/1083/5040/Judiciary%20Launches%20ECCMIS.html#:~:text=On%20Tuesday%20March%201%2C%202022,the%20Judiciary%20Headquarters%20in%20Kampala. On the 20th June 2022.

[26] Hayley Andersen, 'Insights from Africa's COVID-19 Response: Tech Innovations' (December 2020) Research Paper by Tony Blair Institute for Global Change, Pg.3. See also Adyasha Maharana et al, 'COVID-19 and beyond: Use of digital technology for pandemic response in Africa' *Scientific African,* (November 2021, Vol 14)

commerce, policies like embracing digital technology in traditional sectors like agriculture are being promoted.[27] The East African Partner States need to take equally gradual, pragmatic and proactive steps in promoting digitalization within the region with particular regard to regional interests.

The region already has the legal and regulatory structure to coordinate a joint economic effort. The East African Common Market and its regulatory bodies like the East African Competition Authority should be utilized to regulate regional trade. This is particularly importance in regard to digitalization because none of the EAC Partner States alone has the market base to create an attractive digital market.[28] However as a region the EAC as a digital market would be the ninth biggest in the world.[29] At the moment, small scale and medium scale enterprises are being touted as a key for Africa's recovery from the COVID-19 recession.[30] A well-regulated and transparent digital market can leverage on the rising innovativeness and creativity in technology hubs within the region to facilitate entrepreneurship and attract investment.[31]

3. REGIONAL ECONOMY PRIOR TO THE COVID-19 OUTBREAK

The COVID-19 pandemic cannot be said to be the sole cause of the current economic challenges particularly within the East African region. Even prior to the outbreak of COVID-19 many of the EAC Partner States had heavily borrowed. Kenya, Burundi and Rwanda had their Gross Domestic Product (GDP) to debt ratios standing at 62.14%[32], 60.13%[33] and 50.97%,[34] respectively. The borrowing for some Partner States had already exceeded the safe threshold of 50% of GDP in 2019.[35] The Partner States were therefore not in position to counter the pandemic and were running deficit budgets that were highly dependent on tax revenue.[36]

The COVID-19 pandemic disrupted the tourism sector, export trade and income from diaspora thereby gravely undermining the forex reserves of the EAC Partner States. Restrictions and lockdowns that were implemented to counter the spread of the disease undermined local tax revenue. Faced with budget shortages the Partner States were forced to seek more loans. Rwanda, Kenya, Tanzania and Uganda all sought loans to counter the effects of COVID1-19[37].

The picture of the economies of the EAC Partner States before the COVID-19

---

[27] Lurong Chen 'Digital Asia: Facing Challenges from GVCs Digitalisation, US—China Decoupling, and the COVID-19 Pandemic' *Japan SpotLight,* (Dec 2021) Pg.5.
[28] World Bank Group, *Ibid*, Pg.1.
[29] Ibid.
[30] OECD, *Ibid*, Pg.1-12.
[31] World Bank Group, *Ibid*, Pg. 42-50.
[32] AFRODAD, 'Assessment of National Financing and Investment Policies in The East Africa Community (EAC) And Southern Africa Development Community (SADC) Countries Against Regional Protocols' (2019) Pg.12-15.
[33] *Ibid.*
[34] *Ibid.*
[35] AfDB, 'East Africa Economic Outlook 2019: Macroeconomic Developments and prospects Political economy of regional integration' (2019), Pg.8-13.
[36] UNEC, *Ibid*, Pg 4-10.
[37] Berna Namata, 'Huge borrowing, COVID-19 shocks, leave region in a funding dilemma' *The East African*, (05 January 2021) accessed from https://www.theeastafrican.co.ke/tea/business/huge-borrowing-COVID-19-shocks-leave-region-in-a-funding-dilemma-3247156 on the 20th June 2022.

outbreak was that of a region in need of local revenue[38]. The COVID-19 pandemic emphasized this aspect even more. With three out of the Five EAC Partners states with a GDP to debt ration over 50%, the region has to emphasize local revenue as a tool for development and rely less on debt.[39] It is a more sustainable approach for which digitalization is critical because many of the industries that were sources of income tourism will take time to fully recover and the potential of digitalization within the East African Community is yet to be realised. Other Sectors in trade have moved online and it is unlikely that they will revert to the previous mode of operation. The region has moved into a stage where regulation of digital platforms is more critical than it was before.

4. DIGITALIZATION IN THE EAST AFRICAN COMMUNITY

Digitalization refers to utilization of digital technologies to modify an organization's business model and improve ways of delivering services or goods, and the quality of what is delivered.[40] In East Africa, the mobile money revolution in 2007 sparked the process of digitalization .[41] Mobile money enabled financial inclusion by a big number of people who had previously been excluded from basic services.[42] It also created employment opportunities for many both directly and indirectly.[43] Mobile money is credited for helping women access credit and is generally recognized for boosting entrepreneurship in the region.[44]

Currently all the EAC Partner States have a service provider offering mobile money services.[45] As the use for mobile money spread more platforms had to accommodate it both as a means of payment and transaction. This has sparked a spurt of innovations and technological growth not just within East Africa but Africa as a continent. In the past 15 years the growth of digital technology and associated innovations has been one of the bright spots for Africa's development.[46] The technology and innovation hubs that have cropped up in Kigali, Nairobi and Kampala are a reflection digital growth in the East African region.[47] It is anticipated that digitalization can help the African continent as a whole achieve the Sustainable Development Goals faster.[48] That underlines the potential that digitalization has for economic growth the EAC. It is evident that properly managed, digitalization can jump start economies of the EAC Partner States.

In tacit acknowledgement of the potential digitalization The EAC Partner states

[38] UNEC, *Ibid*, Pg 4-10.
[39] Ibid
[40] Ines Mergel, Noella Edelmann and Nathalie Haug,'Defining digital transformation: Results from expert interviews" (2019,Volume 36, Issue 4) *Government Information Quarterly*
[41] World Bank Group, *Ibid*, Pg.27.
[42] OECD, *Ibid*, Pg.41-42.
[43] OECD, *Ibid*, Pg.41-42.
[44] I*bid*
[45] World Bank Group, *Ibid*, Pg.28.
[46] OECD, *Ibid*, Pg.62
[47]*Ibid*, Pg.60-68.
[48] Vera Songwe, 'The Role of Digitalization in the Decade of Action for Africa' *UNCTAD* (07 September 2020) accessed from https://unctad.org/news/role-digitalization-decade-action-africa on the 12th June 2021

in collaboration with UNCTAD[49] launched a task force to guide the Partner states in creating an enabling legal and regulatory environment for digitalization.

The first phase of the work force's activities proposed the enactment of laws regulating Electronic Transactions and Signatures, Cyber Crime, Consumer protection and Data protection[50]. The work force through its activities has created a cohesive legislative foundation regulating digitalization thus far.

4.1. Electronic Transactions and Signatures

The purpose of electronic transactions and signatures legislation was to create a valid and legal means of carrying out business electronically within the East African Community. Without legal recognition, the validity of such transactions can create doubt. This was the issue legislation of electronic transaction and signatures was intended to resolve. Regarding electronic transactions and signatures legislation significant progress has been made. Uganda has already enacted the Electronic Transactions Act,[51] and the Electronic Signatures Act.[52] Kenya enacted the Electronic Transactions Act,[53] which regulates both electronic transactions and electronic signatures. Rwanda enacted the Law Relating to Electronic Messages, Electronic Signatures and Electronic Transactions,[54] which is an ombudsman law governing electronic transactions and computer misuse. Tanzania also enacted an Electronic Transactions Act,[55] governing electronic transactions, signatures and creating legal recognition for online businesses. Because the initiative to enact these laws was started regionally, the legal obligations in the laws are similar,[56] and very little future action will be required to harmonize the laws despite the fact that the Partner States follow the Common Law and Civil Law systems.

4.2. Cyber Crime and Data Protection

The regulation of cybercrime acknowledges that if the electronic platform is to legally use as a transaction platform, then there are people who seek to abuse it or cheat using the same platform. In line with the East African Community Cyber Law task force's recommendations, Uganda enacted a computer Misuse Act[57], Rwanda's Law Relating to Electronic Messages, Electronic Signatures and Electronic Transactions[58] as already discussed above also governs cybercrime. In

[49] UNCTAD, 'Harmonizing Cyber laws and Regulations: The Experience of the East African Community' (2012) Pg.5
[50] *Ibid*, Pg.8 and Pg 52.
[51] The Electronics Transactions Act, 2011.
[52] Electronic Signatures Act 2011 (Act No. 7 of 2011)
[53] The Electronic Transactions Act of 2011(Act No. 8 of 2011)
[54] Law Relating to Electronic Messages, Electronic Signatures and Electronic Transactions Nº 18/2010 Of 12/05/2010
[55] The Electronic Transactions Act (Act No. 13 of 2015)
[56] UNCTAD., "Harmonizing Cyber laws and Regulations: The Experience of the East African Community," 2012, Pg.6.
[57] The Computer Misuse Act, 2011
[58]Law Relating to Electronic Messages, Electronic Signatures and Electronic Transactions Nº 18/2010 Of 12/05/2010.

line with the Task force's proposal Kenya passed the Computer Misuse and Cybercrimes Act[59] and Tanzania passed the Cybercrimes Act[60] to prevent Cybercrime. Just as the case was with electronic signature and transaction laws, regional cooperation has also helped the EAC Partner States have similar cybercrime laws.[61]

It is in regard to data protection that the region is lagging behind in enforcing the task force's recommendations. Only Uganda[62] Rwanda[63] and Kenya[64] have Data protection laws.

4.3. Relevance of the East African Community Cyber Task Force's Approach

The work the task force did in guiding the legislation of E-commerce within the EAC has been commendable. It ensured that the region to a large extent has similar cyber laws and laid an excellent foundation for future cooperation by the EAC Partner States.[65] The task force's efforts are partly responsible for the many cyber laws present in the EAC Partner States.

However, much has changed the task forces' approach may not effectively counter or address some of the new emerging issues. First digitalization within the EAC has progressed tremendously in the past 10 years. There are new emerging fields which are interacting more frequently with East African consumers like cryptocurrency, FINTECH, Data science and artificial intelligence, Global computing and clouding centres, Consumer internet and Internet advertising. Many of these fields are being dominated by global technology giants like Facebook, Google, Twitter, Amazon, eBay most of which are not resident within the East African Community.[66]. In some cases, call have been made for Partner States to legislate certain digital fields like Privacy and data protection on their own because the speed at which the region was proceeding with the legislations exposed consumers to abuse.[67]

None of the individual EAC Partner States have the technical work force and expertise or national market size to effectively compel the Big Tech into compliance with national laws.[68] Furthermore a large section of the EAC Population still has no access to internet.[69] This means a large section of the EAC does not form part of the online market. The approach by the Cyber task force

[59] Computer Misuse and Cybercrimes Act, 2018
[60] The Tanzania Cyber Crimes Act of 2015.
[61] UNCTAD, 'Harmonizing Cyber laws and Regulations: The Experience of the East African Community' (2012), Pg 52.
[62] Data and Privacy Protection Act of 2019
[63] Law Relating to The Protection of Personal Data and Privacy, No. 058/2021 Of 13/10/2021.
[64] Data Protection Act of 2019
[65] UNCTAD, 'Harmonizing Cyber laws and Regulations: The Experience of the East African Community' (2012), Pg.8 and Pg 6.
[66] United Nations Conference on Trade and Development, 'Competition issues in the digital economy' (10-12 July 2019) Note by UNCTAD Secretariat Pg. i-iii, and Pg. 1-5.
[67] National Coalition of Human Rights Defender-Kenya (NCHRD-K), et al 'The Right to Privacy in Kenya: Joint Stakeholder Report Universal Periodic Review 35th Session – Kenya' (July 2019) Periodic review by NCHRD-K, KELIN, Paradigm Initiative, and Privacy International Pg.8, Pg10-11, and Pg 14.
[68] World Bank Group, *Ibid*, Pg.25, Pg. 37 and Pg. 43.
[69] *Ibid*, Pg. 47.

which placed much emphasis on the national governments is currently inadequate. Whereas the EAC Partner States have the capacity to enforce compliance by locally based digital enterprises, the same cannot be said about the global technology giants and non-resident companies. And yet the foreign based global technology giants are in many ways dominant over the East African Region[70]. To better position itself to fully benefit from the developmental effects of digitalization, the East African Community needs to effectively regulate its digital space.

Furthermore, the Cyber Law Task force sought to largely use national legislation as an end in itself. National laws were approached as the final tool to regulating digital activities within the region. This approach is currently inadequate. As pointed out, digitalization has progressed tremendously with many diverse and distinct fields interacting. For instance platforms like Facebook which were once only collecting personal data from users are now also engaged in advertising using the consumers data.[71] Jurisdictions like the European Union utilized existing regional mechanisms to effectively regulate the digital platform and even dominant market players can be effectively monitored.[72] A digital market is the ultimate solution for the EAC as well yet this is not envisioned by the East African Community Cyber Law task force.[73] The situation within the East African Community has changed a lot, foreign global companies have become more dominant over the region, the EAC has a fledgling digital industry that needs support, and numerous avenues for abuse of consumers within the region have emerged within the digital space that the EAC Partner States cannot address on their own.

A nationalist led approach has been ineffective. In fact, it is increasingly exposing the economies of the EAC Partner states to income loss as a result of illicit capital out flows by the non-resident technology companies and foreign online entities and exposing consumers to abuse and fraud. It is evident that whereas regional cooperation has played a role in guiding Partner States on the laws regulating digital plat forms, the implementation and enforcement of the laws is still a national affair and that as a strategy is no longer sustainable.

The nationalistic data protection legislations threaten to even undermine the work East African Community Partner States have achieved in integrating their economies. Regional data protection legislation is one of the areas in which the East African Community is lagging behind as a Regional Economic Community (REC'S). Other REC's, like SADC[74] and ECOWAS[75] have regional laws which in effect provide for the ease of cross border transfer of data in the face of restrictive national legislation.[76]

[70] United Nations Conference on Trade and Development, 'Competition issues in the digital economy' (10-12 July 2019) UNCTAD Pg. i-iii, and Pg. 1-3

[71] United Nations Conference on Trade and Development, 'Competition issues in the digital economy' (10-12 July 2019) UNCTAD Pg. i-iii, and Pg. 1-5.

[72]Anwar Aridi and Urška Petrovčič, 'Big Tech, Small Tech, And the Data Economy What Role for Eu Competition Law?" (2019) World Bank Background Paper Pg.24-32. <https://openknowledge.worldbank.org/handle/10986/33124> accessed on the 20th June 2022.

[73] UNCTAD, 'Harmonizing Cyber laws and Regulations: The Experience of the East African Community' (2012), Pg.8-10 and Pg 52-55.

[74] Southern African Development Community (SADC) Model Law on data protection, 2013.

[75] Supplementary Act A/SA.1/01/10 on personal data protection

[76] Article 43 of the SADC Model Law on Data Protection.

Regional data protection legislation is critical in the East African Community because the data protection legislation of Uganda, Kenya, and Rwanda have data localization requirements and restrict the cross-border transfer of data even to the East African Community Partner States [77]. Uganda and Rwanda in particular have adopted strict data localization requirements in the sector of financial services.[78] It would have been expected for the East African region to be an exception to restrictions on the cross border transfer of data in the data protection legislation of the Uganda, Kenya and Rwanda since the Partner States have committed to the free movement of services[79] and data collection is a service, but this has not been the case. In fact, the restrictions on cross border transfer data are already being felt within the East African region. MTN Rwanda was fined USD 8.5 Million by Rwanda Utilities Regulatory Authority, for transferring and processing its consumer data in Uganda.[80] The decision of Rwanda Utilities Regulatory Authority is an early indication of how data localization requirements and restrictions on cross border transfer of Data threaten to undermine integration within East Africa. Regional legislation is needed to negate the effects data localization requirements and restrictions on cross border data on the East African digital economy. The effect of data localization requirements and restrictions on cross border data transfers within the EAC could be equated to border closures since they bar the cross-border use of data by digital entities thereby depriving them of the full benefits of the East African Common Market.

The Malabo Convention on Cyber Security and Personal Data Protection lists the basic principles on data protection, and these are reflected in the Data protection legislation of Uganda, Kenya and Rwanda.[81] The regional treaty could have been used as tool to limit national restrictions on the cross-border transfer of data if the East African Community Partner States had ratified the treaty. Even though the Malabo Convention stops short of out rightly barring restrictions on cross border transfer of data among member states, Article 14(6) (a) of the treaty prohibits the transfer of data to non-member states unless the State ensures protection of privacy, rights, and freedoms of the persons whose data is being processed. Article 14(6)(a) implies that cross border transfer of data between Member States should not have restrictions. Currently, Rwanda is the only East African Community Partner State to have signed and ratified the Malabo convention. Therefore, the Malabo Convention can only be a guide to the East African region.

[77] Kholofelo Kugler, 'The Impact of Data Localisation Laws on Trade in Africa' (2021) Policy Brief by the Mandela Institute, Pg.2.
[78] Section 68 of the National Payment Systems Act, 2020 of Uganda, and Article 3 of Regulation No.2/2018 on Cyber Security of Rwanda, Article 4 of Law No. 16/2010 of 07/05/2010 Governing Credit Information System of Rwanda.
[79] Article 16 of the Protocol on the Establishment of The East African Community Common Market.
[80] Kholofelo Kugler, 'The Impact of Data Localisation Laws on Trade in Africa' (2021) Policy Brief by the Mandela Institute, Pg.2.
[81] Karishma Banga, Jamie Macleod and Max Mendez-Parra, 'Digital trade provisions in the AfCFTA: What can we learn from South–South trade agreements?' **(**April 2021) Working Paper by *Supporting Economic Transformation,* Pg. 14.

5. NON-RESIDENT ENTITIES IN THE EAST AFRICAN DIGITAL ECONOMY

Whereas the early stages of digitalization in the East African region were dominated by local or resident enterprises.[82] Foreign global companies have increasingly become more dominant in the region as more of the population get access to internet.[83] Using the internet, many non-resident and other foreign companies have managed to project their services within East Africa. Many of the companies do not register or incorporate subsidiaries in the countries in which they offer their services. Any form of registration is often forced upon by operational needs that arise from targeting consumers within the East African Community. Googles need to promote its Africa venture within the East African community for instance forced the company to establish an office in Nairobi.[84]

Ideally technology companies would be welcomed in the EAC because of the opportunities they offer in the form of local employment, and the attraction of expatriates into the country. However, many technology companies are operating within the East African Community through the usage of their applications and websites without registering or incorporating subsidiaries in any of the EAC Partner States.[85] This is made possible through the provision of electronic services like advertising, sales platforms and streaming services that only require internet and no physical presence in a country.[86] The entities in such cases leverage on international brand recognition to market their services. This is a challenge presented by any Non-resident technological entity that has the capacity to project its services in the EAC without the need of registration.[87] The large informal business sector within most East African Community Partner States has exacerbated the problem by creating a convenient setting for unregistered technology companies to operate within the region.[88]

There is currently no specific law in any of the East African Community Partner States that seeks to regulate the registration of online businesses and electronic service providers. As such, there is no specific legal obligation on non-resident technology companies operating online businesses within the East African Community to incorporate locally as is the case with other industries like the Oil and Gas industry. As a result, non-resident technology companies can operate in any of the East African Community Partner States without incorporation or

[82] World Bank Group, *Ibid*, Pg 2.
[83] *Ibid*
[84] Brian Ngugi, 'Google to open Nairobi office for Africa venture' *Business Daily* (16 May 2017) accessed from https://www.businessdailyafrica.com/bd/corporate/companies/google-to-open-nairobi-office-for-africa-venture-2152340 on the 29th of June 2021.
[85] National Coalition of Human Rights Defender-Kenya (NCHRD-K), et al 'The Right to Privacy in Kenya: Joint Stakeholder Report Universal Periodic Review 35th Session – Kenya' (July 2019) Periodic review by NCHRD-K, KELIN, Paradigm Initiative, and Privacy International Pg.8, Pg10-11
[86] *Ibid.*
[87] World Bank Group, *Ibid*, Pg 2.
[88] Christopher Changwe Nshimbi, 'Informality as a Sticky Sector in the Post-Pandemic Era of the Fourth Industrial Revolution' (Volume 2, 2021) *African Journal of International Economic Law* Pg.89-91.

registration. It is a loophole that is being used by many non-resident companies for tax evasion and to avoid regulatory obligations. In such a setting, it is difficult for any of the EAC Partner States to ensure regulatory or even tax compliance of non-resident entities since they are based outside their territorial jurisdiction.[89] This practice also encourages tax evasion since the tax laws often lack enforcement mechanisms to hold non-resident technology companies accountable.[90] Non Resident companies that offer electronic services like data collection ,streaming and online advertising services are the most prominent in this mode of operation and they present an economic challenge that has to be addressed.[91]

By offering services in the East African Community without being held accountable for tax obligations or regulatory breaches, foreign based entities place the Partner States at a distinct disadvantage. They can take full advantage of the infrastructural development of the EAC Partner States, yet they pay no taxes. This is a critical economic challenge because the mode of operation of non-resident technology companies is eerily similar to the Imperial British East African Company that used the railway infrastructure in the region resources from the East African region but offered little in return: an economic partnership in which the East African region was a guaranteed looser. Most importantly, without a recognized legal presence in any of the East African Community Partner States, these non-resident companies cannot be held accountable for their conduct. So far States have reacted to legislative and regulatory breaches by blocking the services of the violating entity and it has proven not to be a sustainable solution.[92]

The issue of non-resident entities operating in EAC States without registration or incorporating subsidiaries is one that has emerged with increased internet penetration within the East African region. Unlike other industries in the East African region like mining, petroleum, tourism and banking where foreign entities need to incorporate subsidiaries within the EAC to trade or provide services, local presence is not necessary with internet-based services. So, whereas the multi-nationals engaged in the petroleum industry within the East African Region like Total, Tullow Oil and CNOOC all have been registered in the EAC Partner States or incorporated subsidiaries, few of the major non-resident technology companies have subsidiaries within the region.[93] It is easier to ensure regulatory and tax compliance with companies that are registered locally therefore than it is with non-resident technology companies.

It is a common phenomenon for instance for the internet to be shut down by countries in Africa during elections or in moments of crisis. Whereas this conduct is easy to dismiss as some form of censorship, that is not entirely the case, it is the reaction of States to entities operating in their countries over which they have no

[89] URN, 'URA to start charging VAT on Facebook, Netflix next month' *The Observer* (20 June 2022) accessed from https://observer.ug/businessnews/74034-ura-to-start-charging-vat-on-facebook-netflix-next-month on the 30th of June 2022.
[90] *Ibid*
[91] *Ibid*
[92]URN, 'Museveni explains why government blocked Facebook in Uganda' *The Independent* (13th January 2021, Kampala) See also, Nduka Orjinmo**,** 'How Nigeria succeeded in clipping Twitter's wings' *BBC News*, (18th January 2022, Abuja) accessed from https://www.bbc.com/news/world-africa-60024742 on the 20th June 2022.
[93] Benjamin Augé, 'Oil and Gas in Eastern Africa: Current Developments and Future Perspectives' (March 2018), Pg 16-21.

control.[94] State sovereignty inherently requires any country to have a substantial amount of control over the activities that happen within its territory, and the reaction of shutting down the internet when they have no control over it is understandable. This has not been helped by the fact that Non-resident Technology entities within the region have exploited their status to operate with total disregard for national laws and regulations.[95]

The ability of Non-resident technology companies to benefit from the regional integration process without investing in it like other local based enterprises presents a challenge and in particular regarding a regional digital market.[96] The integration process favours it members because it is exclusive by its nature.[97] The Members commit themselves to regional economic bloc and offer themselves benefits to which the rest of the world is excluded. These are the benefits that accrue from being a member in a regional economic community.[98] As members of the East African Community Common market unrestricted access to the Common market was one of the benefits that would arise from membership to the EAC[99]. Using the internet, the non-resident technology would enjoy the benefits of a digital market and compete with local enterprises even when they are not based in any of the Partner States. This undermines the EAC and renders the sacrifices the partner States make to sustain the regional bloc almost meaningless. This one major reason why the EAC as a region needs to tackle regional digital trade. The absence of regional regulation of digital platforms has left the region vulnerable.

6. NON-RESIDENT ENTITIES AS A CHALLENGE TO DIGITALIZATION

In all other industries such as oil and gas, mining, agricultural, banking and tourism, multi-national companies have had to either register or incorporate a subsidiary in each of the EAC Partner States in which they are operating.[100] The nature of such industries does not allow them operate businesses remotely or without legal presence in the country in which they are operating because the resources they seek are often within the territory and control of a particular State.

---

[94] Megan Kathure, 'Africa's Digital Sovereignty: Elusive or a Stark Possibility through the AfCFTA?' *Afronomics Law* (16 June 2021) accessed from https://www.afronomicslaw.org/category/analysis/africas-digital-sovereignty-elusive-or-stark-possibility-through-afcfta on the 20th of June 2022. See also URN, 'Museveni explains why government blocked Facebook in Uganda' *The Independent* (13th January 2021, Kampala).

[95] National Coalition of Human Rights Defender-Kenya (NCHRD-K), et al 'The Right to Privacy in Kenya: Joint Stakeholder Report Universal Periodic Review 35th Session – Kenya' (July 2019) Periodic review by NCHRD-K, KELIN, Paradigm Initiative, and Privacy International Pg.8, Pg10-11

[96] Celia Becker, 'Taxing the digital economy in sub-Saharan Africa' *ENSAfrica* (1 December 2021) accessed from Taxing the digital economy in sub-Saharan Africa | International Bar Association (ibanet.org) on the 20th of June 2022. See also Crystal Kabajwara, 'A ray of hope in the new global tax agreement' (19 October 2021) accessed from A ray of hope in the new global tax agreement | Press release (pwc.com) on the 20th June 2022.

[97] James Thuo Gathi, *African Regional Trade Agreements as Legal Regimes* (Cambridge University Press 2011) Pg.190-200.

[98] *Ibid*.

[99] *Ibid*.

[100] Benjamin Augé, 'Oil and Gas in Eastern Africa: Current Developments and Future Perspectives' (March 2018) Pg 16-21.

Compliance with national laws is therefore necessary to exploit the resources in question.

This has not been the case in the digital industry. Most foreign online entities and non-resident entities offer services that do not require their presence in the countries they operate like advertising, entertainment and streaming services. The transactions can be initiated, executed and, contracts performed online within an EAC Partner State but without the knowledge of the State. Even when the transaction involves goods being delivered in Partner State, it is difficult to know that it has taken place, especially when they are not bought in bulk. The income lost in the single items may be negligible, but the total volume of trade can be massive.[101]

The State in these online transactions is at a disadvantage because the major resource it has to offer digital entities is the population with access to the internet and these can already be accessed by both resident and non-resident companies.[102] The threat of losing access to the market as a result of being shut out is the leverage that the States can use to force compliance by non-resident companies.[103] For the leverage to be effective, the State ought to have a substantial market with access to the internet. Countries with large markets like Nigeria have leveraged on their population to ensure that non-resident companies are effectively regulated.[104] The market of the Individual East African Community Partner States is not big enough to secure compliance from non- resident companies, and without regional digital laws, the regional population cannot effectively be utilized by the Partner States to ensure compliance by non-resident companies.

The absence of regional digital laws exposes the EAC Partner States to situations where they must individually counter or regulate numerous non-resident technology companies and yet they lack the leverage to do so. This forms the crux of the challenge that non-resident technology companies present to digitalization in the EAC today. Many non-resident technology companies are dominant are dominant within the EAC and yet they cannot be regulated nationally and are abusing their dominance to operate without adequate regulatory oversight, and this presents numerous challenges.[105]

---

[101] Adegoke Oyeniyi, 'Nigeria captures foreign tech firms in its tax net' *Quartz Africa* (4th March 2022) accessed from Google, Meta and others raise Nigeria prices due to digital tax — Quartz Africa (qz.com) on the 20th June 2022

[102] Celia Becker, 'Taxing the digital economy in sub-Saharan Africa' *ENSAfrica* (1 December 2021) accessed from Taxing the digital economy in sub-Saharan Africa | International Bar Association (ibanet.org) on the 20th of June 2022.

[103] Nduka Orjinmo**,** 'How Nigeria succeeded in clipping Twitter's wings' *BBC News*, (18th January 2022, Abuja) accessed from https://www.bbc.com/news/world-africa-60024742 on the 20th of June 2022.

[104] Opeyemi Bello 'Nigeria's Finance Act 2021 and the Digital Tax Framework: Another Attempt to Boil the Ocean?' *Afronomics Law* (February 1, 2022) accessed from Nigeria's Finance Act 2021 and the Digital Tax Framework: Another Attempt to Boil the Ocean? | Afronomicslaw on the 20th June 2022. See also.
Adegoke Oyeniyi, 'Nigeria captures foreign tech firms in its tax net' *Quartz Africa* (4th March 2022) accessed from Google, Meta and others raise Nigeria prices due to digital tax — Quartz Africa (qz.com) on the 20th June 2022

[105] Celia Becker, 'Taxing the digital economy in sub-Saharan Africa' *ENSAfrica* (1 December 2021) accessed from Taxing the digital economy in sub-Saharan Africa | International Bar Association (ibanet.org) on the 20th of June 2022.

6.1. Regulatory Non-Compliance

The laws governing the corporate entities within the EAC are national in nature. All the EAC Partner States require any entity operating in the country to be either registered as a foreign company[106] or locally incorporated[107]. As a result, many of the multi- nationals operating in other fields like the oil and Gas industry and mining have had to incorporate subsidiary companies to enable them to operate within the EAC.[108]

Regulatory non-compliance by virtue of being non-resident is a legal loophole that is being exploited by non-resident technology companies to the detriment of EAC Partner States. The East African Partner States have a narrow tax base and regulatory compliance is one of the ways the EAC Partner States earn revenue. The cost of establishing a company and regulatory compliance within the EAC is quite high. As a result, many of the EAC countries rank poorly on the World Bank Index regarding the cost of regulatory compliance.[109]

Therefore, any entity that manages to operate within the EAC without being regulatory compliant enjoys a considerable advantage over compliant companies incorporated and registered within the region that are burdened with the regulatory costs. This stifles the growth of the locally based startups since their internet-based competitors would operate without following any of the costly and time-consuming regulatory requirements local enterprises must follow. If anything, it forces startups to establish themselves outside the East African region since they would still be able to enjoy the benefits of accessing the East African market without having to be regulatory compliant. If the region is to create a well-regulated and sustainable digital market, Non-resident technology companies and many informal online entities will have to be reined in and made complaint with national laws or excluded from operating in the market.

Regulatory compliance is key because it enables the Partner States to exercise their own oversight role and ensure that national and consumer interests are protected.[110] By avoiding regulatory compliance mechanisms Non-resident companies facilitate tax avoidance and evasion, anti-competitive practices, undermine consumer redress mechanisms, and stifle the growth of local industries.

6.1.1. Tax Avoidance and Tax Evasion

The laws of Uganda, Kenya, Tanzania and Rwanda require any income made from conducting transaction within the Partner States to be taxed.[111] In view of the

[106] Benjamin Augé, 'Oil and Gas in Eastern Africa: Current Developments and Future Perspectives' (March 2018) Pg 16-21.
[107] *Ibid*.
[108] The National Oil and Petroleum Policy for Uganda Pg-6-9. See also Benjamin Augé, 'Oil and Gas in Eastern Africa: Current Developments and Future Perspectives' (March 2018) Pg 16-21.
[109] World Bank Group, *Ibid*, Pg.33.
[110] *Ibid*, Pg.43-44.
[111] Section 16(2) of the Value Added Tax Act of Uganda, Article 9(d) of The Code of Value Added Tax Law No 06/2001 Of 20/01/2001, Section 46(2)(b) and Section 47 of the Value Added Tax Act Chapter 148 of Tanzania and, Section 8 (2) (d) of the Value Added Tax Act of Kenya, Act no. 35 of 2013.

above provisions, any online transactions in with consumers in any of the Partner States ought to subsequently attract a tax from the entities offering the electronic services.[112]

However, the non-resident technology companies and online enterprises operating in the EAC Partner States do not pay the taxes they incur from their transactions within the region. This is because without local incorporation or registration, legally they do not exist, and such cannot attract tax liability. Yet this does not detract the fact that they carry out transaction and offer services in the very countries in which they do not have legal recognition. Furthermore, the transactions themselves are also difficult to trace since they can be made from online wallets or using credit cards with money being transferred directly to bank accounts outside national jurisdictions.[113] This tax evasion because the entity is legally obliged to pay the tax, but it is exploiting legal loophole to evade the tax.[114]

This is a very unfair trend of events; the foreign companies are using local infrastructure to which they have contributed nothing to conduct business and leaving without making any tax contribution in return. Suffice to note that tax avoidance and evasion are a pervasive vice on the African continent.[115] Given the clandestine nature of the vice, it is difficult to accurate determine the amount of money lost to tax evasion and avoidance. However, estimates indicate that the African region loses approximately 225 billion USD annually due to tax evasion.[116]

Social media taxes that were imposed in Uganda, Kenya and Tanzania were some of the measures that initially taken to make non-resident technology companies tax compliant.[117] Unfortunately, the social media taxes affected the consumers of the services and not the entities providing the services. In Uganda an arrangement has been reached in which electronic service providers including companies like Facebook and Amazon will begin paying Value Added Tax.[118] The same thing was done in Kenya where proceedings from non-resident technology companies now attract VAT.[119] This is an approach similar to that taken by Nigeria where legislation was passed regulating Non-resident companies and detailing

[112] *Ibid*

[113] Celia Becker, 'Taxing the digital economy in sub-Saharan Africa' *ENSAfrica* (1 December 2021) accessed from Taxing the digital economy in sub-Saharan Africa | International Bar Association (ibanet.org) on the 20th of June 2022.

[114]UNCTAD 'Tackling Illicit Financial Flows for Sustainable Development in Africa' (2020) UNCTAD Development Report, 79-90. See Also Abbi M. Kedir, 'Tax Evasion and Capital Flight in Africa' (September 2014) Ajayi, S. I. and L. Ndikumana (Eds.), 'Capital Flight from Africa: Causes, Effects and Policy Issues' (2014) Oxford: Oxford University Press), Pg.6.

[115] Abbi M. Kedir, 'Tax Evasion and Capital Flight in Africa' (September 2014) Ajayi, S. I. and L. Ndikumana (Eds.), 'Capital Flight from Africa: Causes, Effects and Policy Issues' (2014) Oxford: Oxford University Press) Pg.6. See also Spencer. D., 'Capital Flight, Illicit Financial Flows and Cross-border Tax Evasion' (2008) *Tax Justice Network*, 2008.

[116] *Ibid*

[117] Von Lab, 'The Consequences of Social Media Taxes on the Digital Divide' (11 March 2020) accessed from https://www.betterplace-lab.org/the-consequences-of-social-media-taxes-on-the-digital-divide on the 20th June 2022

[118] URN, 'URA to start charging VAT on Facebook, Netflix next month' *The Observer* (20 June 2022) accessed from https://observer.ug/businessnews/74034-ura-to-start-charging-vat-on-facebook-netflix-next-month on the 30th of June 2022.

[119] Opeyemi Bello 'Nigeria's Finance Act 2021 and the Digital Tax Framework: Another Attempt to Boil the Ocean?' *Afronomics Law* (February 1, 2022) accessed from Nigeria's Finance Act 2021 and the Digital Tax Framework: Another Attempt to Boil the Ocean? | Afronomicslaw on the 20th June 2022.

aspects of their tax liability.[120]

In this way it is evident that countries both within and outside the East African community have taken note of the income they lose through non-resident technology companies and initiatives have been taken to reduce this.[121] Many of the national ventures are unfortunately not sustainable, Uganda's mechanism for charging Value Added Tax from electronic service providers for instance lacks avenues for enforcement in the event of none compliance.[122] The difference between the strategy used by Nigeria and Uganda lies in the fact that Nigeria has a large market and the threat of being locked out is enough to ensure compliance sustainably.[123]

The issue of tax evasion has grown tremendously with the emergence of digitalization, so much so that measures been initiated by the International community to address tax evasion and avoidance through the OECD/ G20 Base Erosion and Profit Shifting (BEPS) project.[124] The BEPS project seeks to build an international consensus and use collaboration as a tool to counter tax avoidance, currently Kenya and the Democratic Republic of Congo are the only EAC partner states that are BEPS Framework Members.[125]

The OECD/BEPS framework currently has 144 member states, a testament as to how challenging it has become to regulate Multinational companies in this digital era.[126] The OECD/G20 BEPS project however should not substitute or replace regional ventures particularly within the East African Community. First of all, not all the East African partner states are members. Furthermore, the BEPS framework restricts itself to taxes yet the digital issues affecting the East African Community transcend taxes and include issues like consumer protection, data and privacy protection, digital sovereignty and the protection of local digital enterprises. Any solution the EAC would derive from the BEPS framework would be a partial solution. Most importantly the BEPS framework requires it members to surrender a compromise their fiscal Sovereignty.[127] This would present a problem because digitalization is still emerging within the East African Community and its potential

[120] Opeyemi Bello 'Nigeria's Finance Act 2021 and the Digital Tax Framework: Another Attempt to Boil the Ocean?' *Afronomics Law* (February 1, 2022) accessed from Nigeria's Finance Act 2021 and the Digital Tax Framework: Another Attempt to Boil the Ocean? | Afronomicslaw on the 20th June 2022.

[121] Sissie Fung, 'The Questionable Legitimacy of the OECD/G20 BEPS Project' (December 2017 Vol 2) *Erasmus Law Review* Pg 76-88.

[122] URN, 'URA to start charging VAT on Facebook, Netflix next month' *The Observer* (20 June 2022) accessed from https://observer.ug/businessnews/74034-ura-to-start-charging-vat-on-facebook-netflix-next-month on the 30th of June 2022.

[123] Nduka Orjinmo**,** 'How Nigeria succeeded in clipping Twitter's wings' *BBC News*, (18th January 2022, Abuja) accessed from https://www.bbc.com/news/world-africa-60024742 on the 20th June 2022.

[124] OECD, 'Developing Countries and the OECD/G20 Inclusive Framework on BEPS' (October 2021)
OECD REPORT, Pg. 12-13.

[125] OECD, 'Developing Countries and the OECD/G20 Inclusive Framework on BEPS' (October 2021)
OECD REPORT, Pg. 58-59.

[126] *Ibid*

[127]Sergio André Rocha, 'The Other Side of BEPS: Imperial Taxation and International Tax Imperialism' in Sergio André Rocha and Allison Christians (eds), *Tax Sovereignty in the BEPS Era* (Kluwer Law International BV 2017) Pg.183-185. See also Sissie Fung, 'The Questionable Legitimacy of the OECD/G20 BEPS Project' (December 2017 Vol 2) *Erasmus Law Review* Pg 78.

has not yet been realized. Fiscal policies like tax holidays and tax hikes on non-resident companies are some of the ways to promote local digital enterprises. If EAC Partner States were to surrender their fiscal sovereignty it would limit their ability to adequately protect local companies. Therefore, the OECD/G20 BEPS Framework should form a benchmark and offer guidance to the EAC Partner States as they seek to counter Tax Evasion and Avoidance like it did with the European Union, but it does not have to substitute or limit regional initiatives to regulate the digital sector within the EAC.[128]

6.1.2. Anti-Competitive Practices

Non-resident technology companies also present a challenge to enforcing competition law. Many of the dominant electronic service providers that are dominant within the East African region are non-resident technology companies.[129] These are also in a position to abuse their dominance. In Uganda, for instance, Facebook took the unilateral decision of suspending all accounts that were pro government during the 2021 elections.[130] The decision itself may have been datable but the fact that it was made without adherence to rules of fair hearing that one would expect from a body is not. The Technology giant has been challenged for similar unilateral actions in other jurisdictions like the EU for transferring consumer data to other jurisdictions without prior consent.[131] In Uganda such an avenue for accountability was denied since the company could not be held accountable since they are not incorporated or registered in Uganda as a company or in any other EAC Partner State.[132] The one sided closure of accounts would also amount to abuse of market dominance by discriminating between consumer contrary to the East African Community Competition Act and Uganda's Competition Act.[133] Anti-competitive practices have been associated particularly with dominant technology companies within the European Union (E.U).[134]

The E.U has largely been able to ensure compliance from companies because the dominant technology companies have established themselves within the bloc so as to access its market. The E.U unlike RECS within Africa is therefore in a better

[128] Sissie Fung, 'The Questionable Legitimacy of the OECD/G20 BEPS Project' (December 2017 Vol 2) *Erasmus Law Review*, Pg 76.

[129] United Nations Conference on Trade and Development, 'Competition issues in the digital economy' (10-12 July 2019) Pg.3.

[130] David Vosh Ajuna, 'Pro-govt Facebook accounts in Uganda claim blocking' *The Daily Monitor* (Uganda, 10 January 2021)

[131] Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (C-311/18) See also Dina Srinivasan, 'The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy' (2019, Volume 16 Issue 1) *Berkeley Business Law Journal*, Pg.39-101.

[132] Fred Muwema V Facebook Ireland Ltd [2016] IEHC 519

[133] Sections 8,9,10 and 17 of the East African Community Competition Act. See also Joyce Karanja-Ng'ang'a, 'East African Community Competition Law' In Emmanuel Ugirashebuja (eds), *East African Community Law Institutional, Substantive and Comparative EU Aspects* (Brill 2017) Pg 433-436.

[134] Renda, A., 'Searching for harm or harming search? A look at the European Commission's antitrust investigation against Google' CEPS special Report, September 2015. See also Dina Srinivasan, 'The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy' (2019, Volume 16 Issue 1) *Berkeley Business Law Journal*, Pg.39-101.

position to ensure compliance with its regional laws. The East African Community with an emerging digital industry must take more measures to ensure that its growth is not stifled.

6.1.3. Compromise of Consumer Protection Mechanisms

Non-resident technology companies through legislative and regulatory noncompliance also compromise consumer protection laws and mechanisms. This issue particularly arises with non-resident electronic service providers which acquire access to critical consumer data like addresses and credit card information and the information is exposed or left unprotected.[135] Consumers within the East African region would be forced to seek remedy often in jurisdictions outside the continent for a remedy, they are in essence deprived of a remedy. This can be addressed by a regional legislation requiring all contracts for provision of electronic services within the East African region to have either national courts or the regional court as the first forum of litigation.

As the situation stands, many non-resident companies cannot be sued locally since most do not incorporate themselves locally. East African consumers are deprived of local remedies since without local incorporation such entities cannot be sued. As a result, consumers have to undergo extra cost to acquire remedies. Allowing entities to operate without incorporation deprives the consumers of immediate entity to hold accountable in case of breach.

In one such incident a Ugandan user defamed on Facebook had to file a case in Ireland in a bid to have the identity of the person defaming him disclosed[136]. Consumers are often left to the magnanimity of the online entities they transact with, and this is not sustainable, and it does little to assure consumers about the safety of online transactions. Wariness about electronic transactions is still a challenge to digitalization in East Africa.[137] The absence of accessible means to a remedy is not doing much to ease these fears and consumer wariness in such circumstances is justified.

Fraudulent online entities have already exploited the absence of accountability and remedy mechanisms to scam consumers by utilizing the regulatory supervision over non-resident companies.[138] The result is entities that have trust of consumers continuously abusing the trust without being held accountable. This is possible because some of the digital players have become too big for some states to regulate alone.[139] This is a challenge that has been witnessed, calls have been made for

[135] United Nations Conference on Trade and Development, 'Competition issues in the digital economy' (10-12 July 2019) Pg. Pg. 1-3, and Pg.13.

[136] *Fred Muwema V Facebook Ireland Ltd* [2016] IEHC 519, See also Monitor 'Court orders Facebook to reveal TVO's identity to Muwema' *Monitor* (Uganda, 10 January 2021) accessed from https://www.monitor.co.ug/uganda/news/national/court-orders-facebook-to-reveal-tvo-s-identity-to-muwema-1664308 on the 29th of June 2021.

[137] World Bank Group, *Ibid*, Pg.30.

[138]David Luke and Zodwa Mabuza, 'The Tripartite Free Trade Area and the African Continental Free Trade Area: The Case for Consolidation' United Nationas Economic Commission for Africa (November 2020) Pg. 8. See also Idoot Augustine Obilil, 'Why OneCoin is a ponzi scheme' *Monitor* (03 September 2018) accessed from https://www.monitor.co.ug/uganda/business/prosper/why-onecoin-is-a-ponzi-scheme-1776114 12th June 2022.

[139] United Nations Conference on Trade and Development, 'Competition issues in the digital economy' (10-12 July 2019) Pg. 1-3, and Pg.13.

international response[140] and international measures have already been initiated to counter it.

If the full benefits of digitalization are to be realized, the EAC Partner States have to invest in inspiring consumer confidence in E-transactions. This requires countering and reducing the existing avenues through which online fraud, data theft can be carried out and ease of legally enforcing electronic transactions. The consumers need to have an entity they can hold accountable for contract breaches within reach. A requirement for local registration of all non-resident technology companies would be one of the measures that can be taken.

Furthermore, most electronic service providers acquire consumer data either to provide services or when enforcing payment, in the hands of non-resident companies, this data is not adequately protected by national legislation of the Partner States that have them. Other partner States like South Sudan and Burundi have no data protection laws and this leaves the consumer more exposed to chances of their data being abused. The existing Data protection laws in Uganda, Rwanda and Kenya require entities collecting consumer data to ensure that it is well protected and to restrict the processing of data.[141] In a bid to protect users both the Data protection laws of Uganda and Kenya restrict the transfer of data outside their national jurisdiction.[142] However this protection falls short where the entity collecting the Data is a non-resident technology company already outside the jurisdiction of the Partner State. Such a challenge makes it difficult to monitor consumer data, what it is being used for and renders it impossible to ensure compliance with Data Protection laws. It is paramount that entities that have access to consumer's sensitive information like credit card information are held accountable for what that information is used for and to ensure that it is adequately protected. Such accountability is difficult if the entity is not registered in the consumer's country.

6.1.4. Stifling Local Technology Startups and Business Enterprises

One of the goals of the of the EAC is to promote economic development among the Partner States.[143] To achieve this objective, the Partner States advocate for import duties on certain items like sugar to protect the local industries from external competition.[144] This approach is difficult to implement in regard to digital transactions without existing regional legal framework. The first challenge is the obvious case of non-resident companies whose adherence to tax laws will be low unless an effective means of implementation. Until then, the most useful tool the

[140] United Nations Conference on Trade and Development, 'Competition issues in the digital economy' (10-12 July 2019) Pg. 13.

[141] Sections 18, 25 and 26 of the Data Protection Act of Kenya Act No.24 of 2019 and Sections 9, 11, and 20 of the Data Protection and Privacy Act, 2019 of Uganda.

[142] CIPESA, 'Mapping and Analysis of Privacy Laws and Policies in Africa' (July 2021) Summary Report by Cipesa, Pg. 8. See also Alexander Beyleveld, 'Data Localisation in Kenya, Nigeria and South Africa: Regulatory Frameworks, Economic Implications and Foreign Direct Investment' (March 2022) *Mandela Institute*, Policy Brief No.7, Pg 1-2.

[143] Article 5(3) a of the Treaty Establishing the East African Community.

[144] Dicta Asiimwe and Ismail Ladu, 'Sugar dumping: Uganda, Tanzania want 150pc tariff' *The East African* (Kenya, 11 August 2018) accessed from https://www.theeastafrican.co.ke/tea/business/sugar-dumping-uganda-tanzania-want-150pc-tariff-1400196 on the 29th of June 2021.

region can use to enforce compliance by dominant non-resident companies would be to restriction the access to the East African market.[145] So far, the regional digital market lacks both the legal and regulatory framework, and the infrastructure the utilize the regional market as an implementation tool. So, the local companies are left to compete with dominant non-resident companies without enjoying the full benefits of being resident companies within the region.

Local entities are forced to compete with internationally dominant entities without any form of regional protection and this stifles growth of digital enterprises.[146] The need to protect local startups is one of the reasons countries within the East African region are increasingly localizing Data.[147] The Local startups have the extra burden of having to pay taxes and be regulatory compliant, yet most non-resident technology companies can operate without tax or regulatory compliance. It is a situation that skews the market largely in favour of non-resident technology companies and hamstrings the growth of startups in the region.

Locally based technology companies have been a driving factor of digitalization in East Africa. Through multiple partnerships they have initiated several activities like connecting sub marine internet cables in the East African region[148]. These are infrastructural developments that the Partner States would be hard pressed to invest in on their own, they would not be prioritized and yet they are needed to fully benefit from digitalization. The local entities engaged in these infrastructural projects are deserving of regional protection from international competition to ensure at the very least the investment in digital infrastructure continues. The fact that non-resident technology companies are using existing infrastructure to dominate the local enterprises that are investing in technology infrastructure in the region is a big challenge.

Furthermore, the activities of non-resident technology companies especially the electronic service providers the EAC have had a spillover effect on other traditional industries like television, newspapers and the media industry. Electronic service providers like Facebook have access to consumer data and are in a position to make more targeted advertisements through online advertisements.[149] As a result, they have become a favoured form of advertisement drastically reducing the income of traditional advertising platforms like Televisions and news Papers.[150] In Uganda traditional news outlets that depended on advertisement revenue were forced to launch electronic platforms so as to better compete with social media platforms an yet they are still at a disadvantage because they do not have the reach most dominant non-resident technology companies.

The challenge the East African Community faces with this phenomenon is that the traditional advertising platforms are locally based, pay taxes, are well regulated

[145] Nduka Orjinmo**,** 'How Nigeria succeeded in clipping Twitter's wings' *BBC News*, (18th January 2022, Abuja) accessed from https://www.bbc.com/news/world-africa-60024742 on the 20th June 2022.

[146] CIPESA, 'Mapping and Analysis of Privacy Laws and Policies in Africa' (July 2021) Summary Report by Cipesa, Pg. 8.

[147] *Ibid*

[148] OECD**,** *Africa's Development Dynamics 2021: Digital Transformation for Quality Jobs***,** (2021), Pg.48.

[149] Yan Lau 'A Brief Primer on the Economics of Targeted Advertising' (January 2020) *Federal Trade Commission*, Pg 1-5.

[150] Caroline Kalombe, and Jackson Phiri, 'Impact of Online Media on Print Media in Developing Countries', (January 2019, Issue 4 Vol 7), *Open Journal of Business Management*, Pg.1983, 1992.

and offer employment to citizens unlike the non-resident technology companies they are competing with. A decline in the performance of traditional advertising platforms impacts the national economies through declining local tax revenues and rising unemployment. For the Partner States it is paramount that the entities responsible for this decline in revenue are taxed. At least local platforms of a similar nature should be given a competitive advantage to counter the dominance of the non-resident technology companies in the industry.

7. THE NEED FOR A SINGLE DIGITAL MARKET IN THE EAST AFRICAN COMMUNITY FOR EFFECTIVE REGULATION OF REGIONAL DIGITAL TRADE

The abuse of digitalization by non-resident technology companies and other online based enterprises thus far is largely attributed to the lack of regional laws regulating several digital platforms. The only existing legislations are national laws and regulations, and these cannot adequately counter vices that are transnational in nature. So many online platforms could operate in the region without regard to national regulations with no fear of being held accountable. Unlike countries like Nigeria, the online market size of each of the individual EAC Partner States is negligible and the fear of being closed out cannot compel the non-resident online entities to be legally compliant.[151] A regional digital market in the East African Community would counter all this since it would enable the region to leverage on the East African Community market as a whole. As a region the East African Community is the ninth biggest global market and would be a considerable loss for any entity to be locked out of a market that big[152]. The threat of being shut out of the market would be enough to ensure compliance. The region would be guaranteed to be the winner. The region benefits through creation of employment activities and acquisition of expatriate labour when entities register locally.[153]

A regional digital Market would also come with regulations and laws governing entities operating in the regional market and [154] specialized bodies to monitor the dominance of the major entities in the region to ensure that it is not used to the detriment of the East African Consumers.[155] Both regional legislations regulating online enterprises and regional monitoring bodies are currently absent within the East African community. As a result, East African Consumers are at the mercy of the companies they transact with particularly if they are non-resident companies. This is a dangerous situation for East African Consumers since the motivation for Companies is profit and not the welfare of their consumers.

[151] Nduka Orjinmo**,** 'How Nigeria succeeded in clipping Twitter's wings' *BBC News*, (18th January 2022, Abuja) accessed from https://www.bbc.com/news/world-africa-60024742 on the 20th June 2022

[152] OECD**,** *Africa's Development Dynamics 2021: Digital Transformation for Quality Jobs***,** (2021), Pg.1.

[153] *Ibid*, Pg.15-17.

[154] OECD**,** *Africa's Development Dynamics 2021: Digital Transformation for Quality Jobs***,** (2021), Pg.60-68.

[155] *Ibid*.

7.1. Regional Economic Growth and Regional Cooperation

The mobile money revolution that sparked digitalization within the East African Community made a big impact on the regional economy and made it easy for majority of the population that were not able to access banking services to be financially included.[156] As a result, numerous jobs and opportunities were created. It is anticipated that a regional digital market in the east African community would even have a wider effect. Estimates state that a Single Digital Market in the East African region would boost the regional GDP by up to a US$2.6 billion and create 4.5 million new jobs[157].

The effects of the mobile money so far have largely been felt at a national level. There were many restrictions to monetary transfer between countries that limited the use Mobile Money across countries,[158] and very few mobile money companies operate platforms in more than two East African Countries.[159] To some extent, this has limited the effect and role of the mobile money revolution within the East African regional economy. A Single Digital Market would unlock this potential. For example, it would help the East African region consolidate its efforts to get rid of onerous roaming charges.[160] A single Digital market would also make it possible to de-nationalize data within the East African Community and make it possible to actually transact in data within the region.[161] In this regard, the East African region is being held back by the absence of a legal regulatory framework to enable the establishment of a regional digital market.

Furthermore, Regional Economic Communities were intended to be the building blocks of the African Economic Community.[162] Consensus within the East African Community on the regulation of digital issues could open the field for further cooperation with other Regional Economic Communities. The Tri-partite Free Trade Area was created following the success of the EAC, SADC and COMESA as Regional Economic Communities.[163] The negotiations to establish the Tri-partite Free Trade area equally eased the negotiations to create the Africa Continental Free Trade Area (AfCFTA)[164].

With the ongoing negotiations over the proposed AfCFTA E-Commerce protocol, the East African Community Partner States equally need to priorities the creation of regional legal framework on digitalization. As things stand the East African Community does not have a regional stand some of the critical issues the AfCFTA E-Commerce protocol could potentially address areas like electronic

[156] World Bank Group, *Ibid*, Pg.43.
[157] OECD**,** *Africa's Development Dynamics 2021: Digital Transformation for Quality Jobs***,** (2021),Pg.4 and Pg 77.
[158] OECD, *Ibid*, Pg.4 and Pg 77.
[159] *Ibid*, Pg.4 and Pg. 28.
[160] OECD**,** *Africa's Development Dynamics 2021: Digital Transformation for Quality Jobs***,** (2021), Pg.4 and Pg28.
[161] UNCTAD, 'Harmonizing Cyber laws and Regulations: The Experience of the East African Community' (2012), Pg.8 and Pg 6.
[162] David Luke and Zodwa Mabuza, 'The Tripartite Free Trade Area and the African Continental Free Trade Area: The Case for Consolidation' United Nations Economic Commission for Africa (November 2020) Pg. 1-3
[163] *Ibid*
[164] *Ibid*

trade facilitation, digital business taxation, data protection and privacy , and cross border data flows and storage.[165] If not rectified this could result in a scenario similar to the Malabo Convention on Cyber Security and Personal Data Protection, in which the regional treaty has been ratified by 8 states and only one East African Community Partner State.[166]

It is essential East African Community Partner States come up with legal framework regulating digital businesses within the region since it will guide in negotiating Phase 2 of the Tri-Partite Free Trade Agreement negotiations which involves the regulation of services.[167]

7.2. The Regional Capacity Exists

The developments in digitalization have also come in when the EAC Partner States have signed the Protocol establishing the East African Community Common Market.[168] The East African Competition Act was also passed into law and the East African Competition Authority was commissioned.[169] The EAC Partner States are also co-operating to eliminate roaming charges within the region.[170] There is already a considerable level of collaboration among the EAC Partner States on fields are related to or would directly impact the digital market.

The region should seize the existing cooperation and good will to consolidate the spurt of economic growth that earlier regional integration efforts had sparked. With institutions like the East African Community Competition Authority established to regulate the regional market there is a legal and regulatory basis to compel all companies operating in the region to comply with laws.

This is an excellent platform for the creation of an East African Digital market since the legal framework for the regulation of the regional market has already been established. All that is left is to enact extensive legislations and regulations to cover E-commerce, electronic service providers and all other forms of digital transactions and increase the mandate of the East African Community Competition Authority to cover competition issues within a digitalized economy.

As a region the East African Community can leverage on their population to attract investment, promote local technological start-ups and sustain their growth. This the reason a single digital market is needed in the East African Community. It would be an enabler of many developmental projects and entrepreneurial activities within the region.

---

[165] Karishma Banga, Jamie Macleod and Max Mendez-Parra, 'Digital trade provisions in the AfCFTA: What can we learn from South–South trade agreements?' **(**April 2021) Working Paper by *Supporting Economic Transformation,* Pg. 9-11. See also Kholofelo Kugler, 'The Impact of Data Localisation Laws on Trade in Africa' (2021) Policy Brief by the Mandela Institute, Pg.6-9.

[166] Karishma Banga, Jamie Macleod and Max Mendez-Parra, 'Digital trade provisions in the AfCFTA: What can we learn from South–South trade agreements?' **(**April 2021) Working Paper by *Supporting Economic Transformation,* Pg. 14.

[167] Article 45 Agreement Establishing a Tripartite Free Trade Area Among the Common Market for Eastern and Southern Africa, The East African Community and The Southern African Development Community.

[168] The East African Community Common Market came into force on 1st July 2010.

[169] Joyce Karanja-Ng'ang'a, 'East African Community Competition Law' In Emmanuel Ugirashebuja (eds), *East African Community Law Institutional, Substantive and Comparative EU Aspects* (Brill 2017) Pg 433-436.

[170] OECD, *Ibid*, Pg.4 and Pg 28.

7.3. Registration as a Prerequisite to Access the EAC Digital Market

Having highlighted the challenge that non-resident online entities present in the current East African Community, it is essential that through the East African Community, laws are passed creating a regional digital platform and requiring non-resident online entities to register in any of the Partner states to access the East African regional market. This would ensure regulatory compliance by the different players and stake holders. Other measures such as the use of a requirement for payment to non-resident companies to be made in local banks in a bid to counter tax evasion, improve transparency, and help the region counter money illicit financial out flows through online transactions.

This process need not even wait for the implementation of a single digital market. Using the existing East African Community Common Market protocol such measures can be enforced. Online companies should actually be held liable for activities that constitute an abuse of dominance, including trading without legal or regulatory compliance under the East African Competition Act.[171] The East African Competition Authority should be used as a regional avenue to regulate online businesses where the entity is not incorporated in either Partner State or is too powerful to be regulated by a single state.

CONCLUSION

The COVID-19 Pandemic has unravelled many economies within the East African Community. It is essential for the region to seek new sources of income and reduce the money it keeps losing illicitly. Whereas digitalization and a regional digital market are an avenue through which the region can leverage for post-COVID-19 economic recovery, the field as it currently exists is skewed against the interest of The EAC Partner States. Methodical steps must be taken by the Partner States to ensure that digitalization does not become another avenue through which the region loses money. The nature of digital platforms is such that they facilitate anonymity in certain transactions which can be used for fraud and other forms of illicit monetary outflow. Certain emerging areas like crypto currency are already being linked to illegal trades like human trafficking, drug trafficking and arms dealing. The EAC community needs a regional legal framework to sustainably regulate the digital sector. This is essential not just to counter the emerging economic problems but potentially political issues as well like digital sovereignty. The problems presented by Non-resident technology companies in East Africa have so far superseded the ability of any single EAC Partner State to counter them individually. It is inevitable that they will be in a multi-national setting. The Partner States should either galvanize themselves to counter the issues regionally or wait for consensus at an international level in the form of a treaty. A regional approach offers the EAC Partner States more control over the Digital sector and a better opportunity to steer it in the interests of the region.

[171] Sections 8,9,10 and 17 of the East African Community Competition Act. See Also Joyce Karanja-Ng'ang'a, 'East African Community Competition Law' Pg 433-436.

JUDGES AND TECHNOLOGY: THE TECHNOLOGY QUESTION AND THE KENYAN PRESIDENTIAL ELECTION PETITIONS 2017

Peter Joseph Keya*

ABSTRACT

Technology continues to be adopted in Kenya's electoral process. The Election Act was amended in 2017 to introduce technology in the conduct of general elections. The amendments inter alia established an integrated electoral system that enables biometric voter identification and electronic transmission of results. The Independent Electoral and Boundaries Commission was to procure and put in place the technology necessary for the conduct of a general election and to ensure that the technology in use is simple, accurate, verifiable, secure, accountable and transparent. The presidential election petitions of 2017 provided the first opportunity for the Courts through the Supreme Court to interrogate the technology question as used in the electoral process of a general election. This question manifested itself through the interlocutory and substantive determinations made by the Court in the course of the petitions. Among the measures adopted by the Court included the use of a court appointed IT expert together with an ICT officer, supervision and report by the Registrar of the Court and having the technology question handled concurrently with the main hearing of the petitions. This paper discusses how the Supreme Court handled the technology question its implications. This paper also interrogates the efficacy of the approach taken by the Court and the lessons that can be learnt. It will conclude by suggesting recommendations for future consideration.

* Advocate of the High Court of Kenya with 14 years post admission experience; LLB (Moi University Eldoret); PGD (KSL); LL.M (University of Nairobi); Adjunct Lecturer, Kenya School of Law & Intellectual Property and TMT law practitioner and Election Law litigation expert. This article was developed from a presentation made at the Kenya School of Law's 2nd KSL Annual Conference under the theme: "Lawyers, Constitutionalism and Globalisation", held virtually on 23rd and 24th November 2020. The views expressed are personal and do not necessarily reflect those of any affiliations that the author may be subject to.

INTRODUCTION

From Kenya's electoral history, the place of electoral justice in Kenya cannot be downplayed. The defunct Electoral Commission of Kenya which was the statutory body mandated to oversee the general elections had no clear control of the process. The presidential election was symbolized by the 'winner takes all' principle elevating the stakes of the election to the highest. Previous attempts to challenge presidential elections on account of malpractices did not elicit much as the courts were quick to dismiss them at the slightest of technicalities. In *Kenneth Stanley Njindo Matiba vs Daniel Arap Moi*, challenging the 1992 elections, the first ever petition against the election of the president, the election petition was dismissed on the basis that the Petitioner had not signed the petition personally but through an agent. In the subsequent elections held in 1997, the petition by *Mwai Kibaki v Daniel Arap Moi* against the re-election of the same President Moi met a similar fate on account of lack of personal service on the President, notwithstanding the impracticability of effecting service on a sitting head of state within the statutory timelines. These decisions have since been castigated for creating bad jurisprudence, highly politicized and destined for pre-ordained outcomes.[1] Surprisingly, the following elections in 2002 remain the single most least controversial elections in Kenya's recent history spanning over thirty years as the results were accepted by the individual contestants and the citizens at large.

However, come 2007, the country caught up with its dark past surrounding the general elections when the outcome of that election was bitterly contested. The dispute was mainly by camps belonging to the candidates who had been declared as the winner and runners up. Faith in the Judiciary was no longer there, and the contest spiralled into the populace through calls for mass action and other incidences of violence pitting the state machinery and its candidate on one side and the 'loser' and his supporters on the other.[2] Things quickly escalated culminating into the infamous post-election violence that led to massive displacements of citizens and loss of over 1,000 lives out of the ensuing clashes. It took the intervention of the African Union under its Panel of Eminent Personalities that the dispute was successfully mediated resulting into the Peace Accord.[3] As part of the Peace Accord, the country was to embark on a road map that included addressing the electoral justice. This included the appointment of the Kriegler Commission.[4]

---

[1] Maina Kiai & Anthony Kuria (2008) The human rights dimensions of corruption: linking the human rights paradigm to combat corruption, Journal of Global Ethics, 4:3, 247-253, DOI: 10.1080/17449620802496362

[2]The Chairman of the Electoral Commission of Kenya at the time is reported to have said that he does not know who won that election. This was supported by the Report by the Kriegler Commission.

[3] see also Juma M. K "African mediation of the Kenyan post-2007 election crisis" in *Journal of Contemporary African Studies Volume 27, 2009 Issue 3: Kenya's Uncertain Democracy: The Electoral Crisis of 2008* accessed at https://www.tandfonline.com/doi/abs/10.1080/02589000903187016 and Khadiagala G.M. "Forty days and nights of peace making in Kenya in *Journal of African Elections Vol 7 No. 2 at page 4 accessed at https://www.eisa.org.za/pdf/JAE7.2Khadiagala2.pdf*

[4] Officially known as the Independent Review Committee

In its report, the commission undertook a comprehensive assessment of the electoral process. Among the issues noted, the defunct Electoral Commission of Kenya had no clear control of the election process ranging from the voter register,[5] the proximity of party primaries to the deadline and election date and polling day operations ranging from bribery and abuse of assisted voting, misuse of black books, limited access of agents and inadequate handling of ballots. Unsurprisingly, the report identified problems which were pointers for the need for technology. In its recommendations therefore, the Commission proposed that the counting tallying & announcement of results be incorporated into a policy document, need to develop an integrated & secure data tallying & transmission System, media access to be permitted and time to be given for verifying provisional results.

The raft of measures undertaken involved a wide-reaching public participation. This resulted into another attempt to amend the constitution and resulted to the 2010 national referendum that gave rise to the current constitution, promulgated on 27th August 2020. The first attempt to amend the constitution had been defeated in the 2005 referendum.

2. THE 2010 CONSTITUTIONAL GAINS

The Constitution of Kenya 2010 has been lauded as one of the most progressive pieces of legislation in the world. Its provisions have secured the rights of traditionally marginalized groups including women and youth and it has significantly expanded the space for realization of human rights and promotion of democratic governance.[6] The new Constitution can be appraised as a very modern document, particularly through its Bill of Rights which includes a wide array of socio-economic rights. In this respect, it can be seen from the mere content of the text - alongside the South African Constitution - as one of the most progressive documents on the continent and some provisions in the Bill of Rights develop the South African example even further.[7]

The advent of the new dispensation set in motion the entrenchment of the political and electoral rights. For instance, Article 38 provides for political rights and guarantees the right to free and fair elections[8] as well as the right to be registered as a voter and vote by secret ballot.[9] The electoral body was entrenched as an independent commission under the Constitution[10] and given the responsibility for conducting and supervising elections In a similar manner, Article 86 relates to voting and provides that the Independent Electoral and Boundaries Act (IEBC) should ensure that the voting method deployed should use a system that is simple accurate, verifiable, secure, accountable and transparent. The collation and

[5] The Commission noted that the ECK could not verify the Voter register as it relied on information provided by the voter.
[6] http://creawkenya.org/ke/constitution-reforms-2/
[7] Kenya's New Constitution: A Transforming Document or Less than Meets the Eye? Cornelia Glinz *Verfassung und Recht in Übersee / Law and Politics in Africa, Asia and Latin America* Vol. 44, No. 1 (2011), pp. 60-80 Published by: Nomos Verlagsgesellschaft mbH https://www.jstor.org/stable/43239778
[8] Article 38(2)
[9] Article 38(3)(b)
[10] Article 88

announcement of election results should be by the Presiding and Returning Officer and that structures and mechanisms should be put in place to eliminate electoral malpractice. To operationalise the IEBC and its mandate, Parliament enacted the IEBC Act in 2011[11] whose objective was to make provision for the appointment and effective operation of the Independent Electoral and Boundaries Commission established by Article 88 of the Constitution, and for connected purposes.[12] Section 4(m) of the Act provides that the Commission in performance of its functions to use appropriate technology and approaches.

Parliament also enacted the Elections Act[13] to provide for the conduct of elections to the office of the President, the National Assembly, the Senate, county governor and county assembly; to provide for the conduct of referenda; to provide for election dispute resolution and for connected purposes. The use of technology in elections was introduced through section 44 of the Elections Act and it provided provided that "the commission may use such technology as it considers appropriate in the electoral process."

On the Judiciary front, the Constitution established the Supreme Court as the apex court of the land with the authority to hear and determine certain appeals from the Court of Appeal and whose decisions are binding on all other Courts.[14] Of note is that the Supreme Court was clothed with exclusive original jurisdiction to hear and determine disputes relating to the elections to the office of President arising under Article 140.[15] The Court was also given a constitutional timeline of fourteen days from the date of filing of the petition within which to hear and determine the petition challenging the validity of the election of president.[16] To avoid a recurrence of the 2007 post-election violence and in conformity with the transformation within the Judiciary, an effective and efficient Electoral Dispute Resolution process was established in the run up to the 2013 General Election. The Judiciary established a temporary committee – the Judiciary Working Committee on Election Preparations in May 2012 – to, among other things: advise the Judiciary on administrative arrangements and measures for the efficient disposal of election related disputes; design and execute a Judiciary programme to build the capacity of Judges, Magistrates and other Judicial Officers on electoral matters; design a system for monitoring and evaluating the management of election related disputes in court; liaise with and coordinate stakeholders to ensure effective and timely resolution of election related disputes and offences as well as advise the Judiciary on public outreach strategies on the election process.[17]

3. THE 2013 ELECTION

This was the first test for the use of technology in the elections. Technology was adopted in the electoral process to a certain extent involving voter identification exercise and in the electronic transmission system. However, during the tallying

[11] Act No.9 of 2011
[12] Long title to the Act
[13] No.24 of 2011
[14] Articles 163(3) to (7)
[15] Article 163(3)
[16] Article 140(2)
[17] https://www.judiciary.go.ke/about-us/our-programmes/judiciary-committee-on-elections-2/

process, there was a failure of electronic results transmission system which left the IEBC no other option but to resort to manual tallying of results resulting to an inability by IEBC to declare results as and when they were available. As a sign of the improved confidence in the judicial process, petitions challenging the election of president were filed at the Supreme Court. The petitions were consolidated and heard concurrently owing to the limited constitutional timelines within which to hear and determine the petitions once filed.

Several issues relating to technology were raised both in the pleadings and in the arguments. Among them was the procurement of the devices used where it was argued that the IEBC had violated the Constitution and the Public Procurement and Disposal Act by awarding the tender to an unqualified bidder who then supplied devices that did not work properly or simply failed on the material day.[18] It was further argued that the electronic systems acquired and adopted by IEBC to facilitate the general elections were poorly designed and implemented and destined to fail. IEBC was therefore unable to transmit results of the elections in contravention of Regulation 82 of the Elections (General) Regulations, 2012. A further argument was made to the effect that that there had been inconsistent application of electronic devices and abandonment of such technology with IEBC resorting to manual electoral procedure. The highlight of this petition was that the attempt by the main presidential contestant aggrieved by the election result to file the 900-page affidavit was unsuccessful.[19] This prevented the Judges from considering the contents and it can only be extrapolated that the affidavit contained further evidence on the use /and or failure of technology deployed in the elections.

The Court underscored the use of technology in the election in the following manner:

> [4] The elections of 4th March, 2013 were the first in Kenya to attempt to use electronic facilitation. The IEBC, at various stages of the election, deployed the following technologies: (i) Biometric Voter Registration (BVR) during voter registration; (ii) Electronic Voter Identification (EVID) on polling day; and (iii) Results Transmission System (RTS) during tallying.

In the end, the Supreme Court held that IEBC was entitled to resort to the use of the manual tallying system as the Constitution and Election laws specifically give IEBC discretion to either work with a full electoral system or a manual system. This is the import of section 44 of the which provided that *the commission may use such technology as it considers appropriate in the electoral process.* The Court further found that the evidence on record portrayed that the tallying was indeed conducted in accordance with the law. This was due to inherent failure of electronic systems, the manual tallying not having been challenged. The learned Judges expressed themselves as follows:

> [233] We take judicial notice that, as with all technologies, so it is with electoral technology: it is rarely perfect, and those employing it must remain open to the coming of new and improved technologies.

[18] Paragraphs 12, 14 and 18 of the Judgment in *Raila Odinga & 5 Others v Independent Electoral and Boundaries commission & 3 others* [2013] eKLR.
[19] Ruling on affidavit dated 26th March 2013

> [237] From case law, and from Kenya's electoral history, it is apparent that electronic technology has ***not*** provided perfect solutions. Such technology has been inherently undependable, and its adoption and application has been only *incremental*, over time. It is not surprising that the applicable law has entrusted a *discretion* to IEBC, on the application of such technology as may be found appropriate. Since such technology has not yet achieved a level of reliability, it cannot as yet be considered a permanent or irreversible foundation for the conduct of the electoral process. This *negates the Petitioner's contention* that, in the instant case, *injustice, or illegality in the conduct of election would result, if IEBC did not consistently employ electronic technology*. It follows that the Petitioner's case, insofar as it attributes nullity to the Presidential election on grounds of failed technological devices, is not sustainable.

In essence, the Judges appreciated that technology in its all facets was not perfect and was bound to fail at any given point. The IEBC was accordingly excused for its conduct to the extent that IEBC was found to have the discretion to resort to manual or technology electoral system. The judges were satisfied with the evidence on record which to their opinion portrayed that the tallying was indeed conducted in accordance with the law. The judges saw no need to make any further inquiry into the technological aspects of the elections and entirely relied on the positions advanced by the antagonists in the dispute before the Court. Consequently, the election was held to be valid, and the petitions dismissed. It is also worth noting that the Court did not delve into the legality or motive of the procurement process as had been advanced pointing to a predetermined failure of the technology deployed.

4. POST-2013 DEVELOPMENTS

Following the said 2013 elections and the determination by the Supreme Court, several concerns were raised some of which led to legislative amendments. These concerns included verifiability, perceptions that technology equals credibility of elections and the fears of the voting by the so called "dead voters." Further changes to the electoral laws were affected following the recommendation of a Bi-Partisan Joint Parliamentary Committee. The various amendments to election law, geared towards enhancing the conduct of free and fair elections, were made. They included sections 39 and 44 of the Elections Act which were amended to provide for the manner in which Presidential election results would be declared and published after close of polling and the introduction of the use of technology in transmission of results. That Regulation 79 of the Elections (General) Regulations as amended[20] also introduced statutory Forms 34A, B, and C for the purposes of declaration of presidential election results while regulation 83 was amended to introduce the provision that the Chairperson of the IEBC shall tally and verify the results at the NTC[21]. The KIEMS system to be introduced under Section 44 further had a complementary manual system, which was upheld by the Court of Appeal in

[20] by Legal Notice No.72/2017
[21] Regulation 83(2)

the case of *National Super Alliance (NASA) Kenya v. The Independent Electoral and Boundaries Commission & 2 Others*.[22] The above reforms were made in an effort to ensure that the technology, restricted to biometric voter registration, biometric voter identification and electric result transmission system, would pave way for free and fair elections administered in an efficient, simple, accurate, verifiable, secure accountable and transparent manner.

In summary as at the time of conducting the 2017 elections, the laws now provided for the procurement of technology 120 days before the election[23] requirement for regulations on technology within commencement of the section, the establishment and mandate of the Electoral Technology Advisory Committee including the representation by political parties, the testing of technology within 60 days to the general election, technology related offences and complementary mechanism for voter identification and results transmission.

The Elections(Technology) Regulations, 2017 were also enacted to provide for the establishment of a framework governing the use of election technology including establishment of a public web portal for public inspection of the voter register; operational aspects of the transmission of results; the assessment, procurement, deployment, maintenance and disposal of election technology assets; certification of the election technology; data retention and disposal; audit of the election technology; development and testing of an operations continuity plan and data recovery mechanisms in case of technology failures and establishment and functioning of the Election Technology Advisory Committee.

The important sections to note regarding the use of technology particularly in presidential elections are sections 39, 44 and 44A of the Elections Act. This paper highlights the sections as they were at the time of elections in August 2017 and do not extend to any post-election amendments that may have been made to the provisions.

4.1. Section 44 Elections Act

This is the section that deals with the use of technology in elections. Section 44(1) established an integrated electronic electoral system that enables biometric voter registration, electronic voter identification and electronic transmission of results. The said system must be simple, accurate, verifiable, secure, accountable and transparent. Under section 44(7), the technology to be used for the purpose of the general election in 2017 was restricted to the process of voter registration, identification of voters and results transmission, and was to be procured at least 120 days before the election.

As per the statutory amendments, the registration of voters must be biometric, and the identification of voters on the voting day and transmission of results should be electronic. The several timelines introduced could not be all been met due to several challenges including numerous suits instituted against the IEBC prior to the 2017 election. This section required consultations by stakeholders including political parties in the coming up with regulations to implement the provision of this section on the acquisition, adoption and use of technology. The law now contemplated the establishment of the Technical Committee of the IEBC consisting

[22] [2017] eKLR Petition No.328 of 2017
[23] One year for others

of such members and officers of the Commission and such other relevant agencies, institutions or stakeholders as the Commission may consider necessary to oversee the adoption of technology in the electoral process and implement the use of such technology. There is also the Elections Technology Advisory Committee with its role and mandate set out in law.[24]

4.2. Section 44A Elections Act

This provision was introduced in January 2017 to address the complementary mechanism for the identification of voters.[25] The section provides that:

> Notwithstanding the provisions of section 39 and section 44, the Commission shall put in place a complementary mechanism for identification of voters and transmission of election results that is simple, accurate, verifiable, secure, accountable and transparent to ensure that the Commission complies with the provisions of Article 38 of the Constitution.

The section was amplified in the Elections (General) Regulations 2017,[26] to provide for the complimentary mechanism for identification of voters at polling stations in the following manner:

- The Presiding Officer is to invite agents and candidates to witness that voter cannot be identified using the device.
- He/she completes verification Form 32A in their presence
- He/she identifies voters using the printed register
- Once identified, he/she issues the voter with ballot paper
- At the end of voting and before counting of ballots in their presence, he/she must enter into the polling station diary the number of persons identified using the printed register of voters

From this provision, it was evident that the only complementary mechanism covered is limited to voter identification. The bone of contention was argued and brought out in High Court at Nairobi decision in *NASA vs IEBC & 2 others* (supra) which was upheld by the Court of Appeal. These issues found their way in the subsequent petitions challenging the presidential elections held in the 2017 general elections. Considering that the register of voters was supposed to contain biometric data[27] and that the identification of voters has to be electronic and based on biometric data, it is unclear as to whether the complementary mechanism as adopted by IEBC was sufficient in the circumstances. The process set out in Regulation 69 was also likely to be challenged on whether it amounts to what is contemplated. It was hitherto unclear what form the biometric identification would take and to what extent this amendment addressed the initial concerns[28] that resulted to the use of technology in the electoral process. For instance, some agents may collude with the presiding officer in aid of a candidate fill the requisite forms

[24] Established under section 44(8) of the Elections Act
[25] Vide section 19 of Act No.1 of 2017
[26] Through regulation 69 thereof
[27] Regulation 8 of the Elections (Registration of Voters) Regulations
[28] From the Kriegler Commission Report and the 2013 elections as captured in the Supreme Court's judgment

and purport that the identification device failed to identify and end up voting for dead or absent voters where the voter turnout is low.

The issue arising from this provision is the term and place of the word "complementary' as used in the section. Was it to be an alternative? Was it to be back-up or was it in addition to? The interpretation of this word in its context was always going to be key on the determination of the applicability of the said mechanism adopted by IEBC, the Supreme Court decision in 2013 having affirmed that the IEBC had some latitude in applying the statutory provisions.

4.3. Section 39 of the Elections Act

This section deals with the determination and declaration of results. For purposed of presidential election and use of technology, section 39(1C) provides that IEBC shall:

> a) Electronically transmit, in the prescribed form, the tabulated results of an election for the President from a polling station to the constituency tallying centre and to the national tallying centre;
>
> . . .
>
> c) Publish the polling result forms on an online public portal maintained by IEBC."

Section 39 also provides for the role of the constituency returning officers responsible for the collating and announcing the results from each polling station in the constituency for the election of the President and submitting, in the prescribed form, the collated results for the election of the President to the national tallying centre. The role of the constituency returning officer in the declaration of results for the presidential election was subject to litigation all the way to the Court of Appeal in *Independent Electoral & Boundaries Commission v Maina Kiai & 5 Others*.[29] This issue was likely to find its way back in court whereby the role of the Chairman of IEBC as the returning officer for presidential election vis-a-vis that of constituency returning officers in the respective constituencies.

There remained a potential lacuna in the law as to the transmission of the results considering that the law was only express as the IEBC on the complementary mechanism for voter identification, there being no such express provision in relation to electronic transmission of results. This afforded some discretion to IEBC as earlier mentioned. As is accepted, technology is not perfect and in susceptible to failure. The law does not therefore contemplate failure in the electronic transmission of results system. In the event that there is any such failure in the electronic transmission process, then whichever mechanism that IEBC resorts to is subject to challenge as to whether it is in conformity with the law.[30]

Following the conclusion of the 2013 EDR process and ahead of the 2017 general elections, the election committee was made a permanent Committee of the Judiciary and renamed the Judiciary Committee on Elections in August 2015 by

[29] [2017] eKLR Civil Appeal No.105 of 2017

[30] In the 2013, there were concerns as about half (17000 of 33000 polling stations managed to transmit provisional results electronically)

the then Chief Justice Dr. Willy Mutunga. The Judiciary Committee on Elections was launched in August 2015, as a standing committee to provide a mechanism to assist the Judiciary prepare for and discharge its mandate on election dispute resolutions.[31] The Judiciary was now under new leadership led by Justice David Maraga as the Chief Justice[32] and Lady Justice Honourable Philomena Mwilu as the Deputy Chief Justice[33] all of them having come from the Court of Appeal ranks. Justice Isaac Lenaola had also been elevated to the Supreme Court from the High Court where he had established himself in the Constitutional Review decision and was well versed in matters involving the interpretation and application of the Constitution[34]. The new judiciary leadership had assumed office barely a year before the elections. This followed the exit of Chief Justice Dr. Willy Mutunga who had opted to retire one year earlier to allow a new Chief Justice to take over the reins in good time for the 2017 general elections.[35] The then Deputy Chief Justice and one other Judge of the Supreme Court, Justice Philip Tunoi had also retired following attainment of the retirement age, their legal challenge to the said case having borne no fruit after the Supreme Court declined to entertain the case.[36] Following the 2013 election cycle, the Judiciary had revamped itself to be better prepared for handling electoral disputes.

5. THE 2017 GENERAL ELECTION

The general election of 2017 was also held for the first time under an elaborate regime of electoral laws including amendments to the Elections Act made to introduce the Kenya Integrated Electoral Management System which was a new devise intended to be used in the biometric voter registration, and, on the election day, for voter identification as well as the transmission of election results from polling stations simultaneously to the Constituency Tallying Centre and the National Tallying Centre. The membership of the Independent Electoral and Boundaries Commission, had also been changed barely seven months to the general election[37]. As the Supreme Court was later informed, the above reforms were made in an effort to ensure that the technology, restricted to biometric voter registration, biometric voter identification and electric result transmission system, would pave way for free and fair elections administered in an efficient, simple, accurate, verifiable, secure accountable and transparent manner[38]

---

[31] https://www.judiciary.go.ke/about-us/our-programmes/judiciary-committee-on-elections-2/

[32] https://www.theeastafrican.co.ke/news/2558-3422436-by69rxz/index.html

[33] https://www.president.go.ke/2016/10/28/lady-justice-mwilu-sworn-in-as-deputy-chief-justice/ see also https://allafrica.com/view/group/main/main/id/00046843.html

[34]https://www.eac.int/press-releases/602-1044-859-eacj-congratulates-the-deputy-principal-judge-justice-isaac-lenaola-upon-his-new-appointment-as-judge-of-the-supreme-court-kenya

[35] https://www.the-star.co.ke/news/2015-03-26-chief-justice-willy-mutunga-to-retire-early/

[36] *Lady Justice Kalpana H. Rawal & 2 others v Judicial Service Commission & 6 others* [2016] eKLR see also https://citizentv.co.ke/news/supreme-court-rules-against-dcj-rawal-judge-tunoi-in-retirement-case-130379/#:~:text=DCJ%20Rawal%2C%20Justice%20Tunoi%20to%20retire%20at%2070&text=The%20Supreme%20Court%20has%20upheld,once%20the%20court%20is%20reconstituted.

[37] Despite the warnings from the Kriegler commission not to have such changes too close to a general election

[38] Paragraph 108 in the majority judgment Raila Amolo Odinga & another v Independent Electoral

This again proved not to be a perfect election despite all the efforts to deploy appropriate technology. The pointer to this state of affairs and the technological battle front was the press statement issued soon after the declaration of the presidential results by the National Super Alliance Coalition (NASA) leader and presidential contestant, Raila Odinga who had yet again come second in the 2017 president election contest. In the highly anticipated address to the press, he termed the results as "*vifaranga vya computer*" loosely translated from Kiswahili national language as "computer generated chicks (leaders)". The NASA leader decried what he described as 'glaring fraud with the results transmission system' setting the stage for his rejection of results and the subsequent resolution to move to the Supreme Court to challenge the results of the presidential election.[39] While many Kenyans found the statement funny and shared light moments through the twitter platform using the hashtag "#vifarangavyacomputer,"[40] the battle lines had been drawn and in another show of confidence in the Judiciary, it was evident that Supreme Court was expected to decide on the otherwise complex question of technology.

5.1. The 2017 Presidential Election Petition and the Technology Question

On the last day within which to file the election petition challenging the election of the president[41], Raila Odinga lodged his petition[42] as he personally escorted his legal team to the Court. His running mate and deputy presidential candidate Kalonzo Musyoka was the co-petitioner. The petitioners in the petition averred that the Independent Electoral and Boundaries Commission, conducted the election so badly that it failed to comply with the governing principles established under Articles 1, 2, 4, 10, 38, 81, 82, 86, 88, 138, 140, 163 and 249 of the Constitution of Kenya and the Elections Act.[43] Their petition was anchored on the grounds that the conduct of the 2017 presidential election violated the principles of a free and fair election as well as the electoral process set out in the Constitution, electoral laws and regulations and that the respondents committed errors in the voting, counting and tabulation of results; committed irregularities and improprieties that significantly affected the election result; illegally declared as rejected unprecedented and contradictory quantity of votes; failed in the entire process of relaying and transmitting election results as required by law; and generally committed other contraventions and violations of the electoral process.[44]According to them, this failure was deliberate, systemic and systematic.

---

and Boundaries Commission & 2 others [2017] eKLR

39 Sara Okuoro "How Kenyans reacted to Raila's announcement on NASA next move" in the Standard Newspaper, August 16th, 2017, edition. Story accessed at https://www.standardmedia.co.ke/kenya/article/ 2001251600/how-kenyans-reacted-to-raila-s-announcement-on-nasa-next-move. See also the live address on https://www.youtube.com/watch?v=m0iTJ24BxKE

[40] KOT react hilariously to Raila's 'vifaranga vya computer' mic drop by ERIC MATARAAugust 16th, 2017 accessed online at https://nairobinews.nation.co.ke/news/railas-vifaranga-vya-computer-jibe

[41] 18th August 2017 being the 7th day after the declaration of the Presidential election results on 11th August 2017 as per the provisions of Article 140(1) of the Constitution.

[42] Supreme Court Petition No.1 of 2017

[43] Paragraph 6 of the majority decision

[44] Paragraph 14 of the majority decision

In the petition, the petitioners having raised several issues of discrepancies in the results declared in the forms 34B as against those forms in the KIEMS portal as against those results in Forms 34A, they had sought an order for scrutiny and audit of rejected and spoilt votes, scrutiny and audit of all the returns of the presidential election including but not limited to Forms 34A, 34B and 34C and scrutiny and audit of the system and technology used by IEBC in the presidential election including but not limited to the KIEMS Kits, the Server(s); website portal.

Subsequent to the filing of the petition the petitioners filed an application[45] seeking among others the following orders:

> …
>
> 3. This honourable court be pleased to order the 1st respondent to give access to the petitioner/applicant to the following:
>
> a) Direct, unfettered access to relevant persons and systems at Safran in order for the forensic information technology experts to fully understand the KIEMS system.
>
> b) Full and unfettered physical and remote access to each biometric electronic appliance used at each voting/polling station location used to verify voters IP voters' identification against the list of registered voters and for the appliances to be forensically imaged to capture, inter alia, metadata such as data files, creation ties and dates, device IDs MAC addresses, IP.
>
> c) Addresses, geographic and local communications mast information.
>
> d) Full and unfettered physical and remote access to any local server(s) connected to the electronic device(s) used to verify voters' identification against the list of registered voters at each polling station, from which a forensic image will be taken.
>
> e) Electronic device(s) used to capture Form 34A's and Form 34B's onto the KIEMS system and transmitted to a) the CTNs and b) the NTC.
>
> f) Full and unfettered access to any form of scanning device which saved images onto access to any form of scanning device which saved images onto an access local server(s) for onward transmission.
>
> g) Access to any scanning device which would serve to establish whether the Form 34A was captured, stored and forwarded in the expected timeframes.

[45] dated 25th August 2017 premised on Articles 19, 20, 22, 23(3), 35, 81, 86, 140, 159 and 258 of the Constitution, Section 39 and 44 of the Elections Act, Section 27 of the Independent Electoral and Boundaries Commission Act, Sections 12, 23 and 26 of the Supreme Court, Rule 18 of the Supreme Court (Presidential Election Petition) Rules, Access to Information Act and the Elections (Technology) Regulations

h) Full and unfettered physical and remote access to any server(s) at the CTNs for storing and transmitting voting information.

i) Full and unfettered physical and remote access to any servers at the NTC for storing and transmitting voting information.

j) Addresses, source and destination IP Addresses, server details and user details.

k) Full and unfettered to access to all source codes, including all programming codes, pursuant to The Election Regulation Technology, 2017.

4. This honourable court be pleased to order the 1st Respondent to give access to all Parties, the following information and data that is in the exclusive possession:

a) The IEBC Election Technology System Network Architecture for the period of 30 days before the elections to the date of the Order of this Court comprising but not limited to:

i. all the servers used during the Elections;
ii. number of servers;
iii. location of servers;
iv. firewalls;
v. IP addresses;
vi. Operating systems;
vii. Software running applications

b) The IEBC Election Technology System Redundancy Plan comprising but not limited to:

i. Password policy;
ii. Password matrix;
iii. Owners of system administration password(s)
iv. System users and levels of access

c) The IEBC Election Technology System Redundancy Plan comprising:

i. Business continuity plan;
ii. Disaster recovery plan.

d) Certified copies of certificates of Penetration Tests conducted on the IEBC Election Technology System prior to and during the 2017 General and Presidential Election including:

i. Certified copies of all reports prepared pursuant to Regulation 10 of the Elections (Technology) Regulations, 2017; and
ii. Certified copies of certificate(s) by a professional(s) prepared pursuant to Regulation 10(2) of the Elections (Technology) Regulations, 2017.

e) In relation to KIEMS Kits:

i. Import testing certification in relation to all KIEMS Kits;
ii. Static IP addresses of each KIEMS Kit used during the Presidential Election;
iii. Specific GPRS location of each KIEMS Kit used during the Presidential Election for the period between and including 05th August 2017 and 11th August 2017;
iv. Certified list of all KIEMS Kits procured but not used and/or deployed during the Election;
v. Polling station allocation for each KIEMS Kit used during the Presidential Election;
vi. Audit log of what each KIEMS Kit used during the Presidential Election transmitted from Polling Stations to Constituency Tallying Centres and to IEBC National Tallying Centre; and from IEBC Result Transmission Database to Media Houses Application Protocol Interface (API) (logs of media data update). Log must also show:

- Time of transmission from KIEMS Kit to the IEBC Result Transmission Database; and
- Time of transmission from IEBC Result Transmission Database to the Media Houses API;
- Count of Identified Voters by each KIEMS Kit;
- Soft copy of Ids captured in each KIEMS Kit;
- Audit log of transmission of scanned Forms 34A from each of the KIEMS Kits.

f) Technical Partnership Agreement(s) for the IEBC Election Technology System including but not limited to:

i. List of the technical partners;
ii. Kind of access they had;
iii. List APIs for exchange of data with the partners;

g) Log in for the period of 30 days before the elections to the date of the order of this court of trails of showing the trail of users and equipment into all the IEBC Servers.

h) Log in for the period of 30 days before the elections to the date of the order of this court of trails of users and trails of users and equipment into the KIEMS Database Management Systems.

i) Administrative access log into the IEBC public portal between 5th August 2017 to date.

5. The 1st Respondent be compelled to give access to and supply to the court and to the Petitioners for scrutiny, certified photocopies of the original Forms 34A's

34B's and 34Cs prepared at and obtained from the polling stations by Presiding Officers and used to generate the final tally of the Presidential election, and pursuant to such production leave be granted for the use of an aid or reading device to assist in distinguishing the fake forms from the genuine ones.

6. The 1st Respondent be compelled to give the Petitioners access Form 34A's 34B's and 34 C's from all 40,800 polling stations.

7. This honourable court be pleased to grant leave to the Petitioner/Applicants to:

    a) Rely on and or file further affidavits in support of the petition and or the affidavits of (i) Rt. Hon. Raila Amolo Odinga, Omar Yusuf Mohamed, (ii) Omar Yusuf Mohamed, (iii) Dr. Edga Ouko Otumbo, Nyangusi Oduwo and (iv) Norman Magaya dated 24/8/2017 be admitted on record and or be deemed to have been properly filed.

    b) File such other affidavits in response to or reply to any responses filed by the respondents.

8. This Honourable Court be pleased to grant any other reliefs that become just and fit to grant.

In that regard, the applicants contended that the Elections Technology System was *"penetrated and/or deliberately compromised and used in a manner not intended by law so as to interfere with and affect the result of the Presidential Election."*[46] They also contend that prior to 8th August 2017, the IEBC deliberately refused to respond to or accede to numerous requests that were made by NASA through its Chief Executive Officer, Mr. Magaya, and its agents. It is their further contention that the information and data that is sought is critical to demonstrate that the 1st Respondent did not conduct a free, fair, secure, verifiable, accountable and transparent election. Further, that the end result, in their view, was that the evidence adduced, points to indicators of interference with the KIEMS system, fraud in the filing of Forms 34A, 34B and 34C and the KIEMS system was not secured as by law required. It is their other view that the said system was breached and/or deliberately compromised and used in a manner not intended in law. That therefore a scrutiny of the IEBC System logs and return is imperative.[47]

As expected, the application was vehemently opposed by the respondents the IEBC and its Chair maintaining that they had at all times followed the law. As anticipated, they argued that they retained discretion as to which method of complementary mechanism to deploy provided that it was simple accurate verifiable and transparent.

The application was canvassed orally before the Judges as the same had to be determined at a preliminary stage. Following their deliberations, the Supreme Court issued a ruling partially allowing the application. This was a stark departure from the Court's ruling in 2013 where it declined an application to compel IEBC to

[46] Paragraph 7 of the ruling in Raila Amolo Odinga & another v Independent Electoral and Boundaries Commission & 2 others [2017] eKLR
[47] Ibid at paragraph 12

deliver to the court and to all the parties herein**,** within Twenty Four (24) Hours of making of the orders all information, electronic and hard copy, in relation to the just concluded Presidential Elections within their power, possession, control and/or custody and to facilitate a Forensic Audit of the First Respondent's IT System prior to the hearing of the Petition. The application in the 2013 petition also sought an directing IEBC, its Servants, Contractors, Agents and/or Service Providers including Kencall EPZ Limited, LANtech (Africa) Limited, Face Technologies, Next Technologies and Google Kenya Limited to deliver to the court and all the Parties herein within Twenty Four (24) Hours of making of the order, all information, electronic and hardcopy in relation to the just concluded Presidential Elections that are within their power, possession, control and/or custody and more specifically the information, devices and appliances listed to facilitate a Forensic Audit of the First Respondent's IT system prior to the hearing of this Petition. The specific devices and appliances to be produced are listed in sub- paragraphs "a" to "u" of paragraph Two (2) of the Application.[48]

The Court this time round allowed access to and scrutiny of forms 34A, 34B and 34C used in the presidential election, as well as access to certain information relating to the IEBC's electoral technology system. The exercise of access was to be conducted under the direction of the Registrar of this Court, two ICT experts appointed by this Court with each of the principal parties being represented by initially two and later, five agents. The reports from that exercise were to be filed in Court. The court summed up the application as seeking three main prayers - access to information relating to the hardware and software used in the conduct of the Presidential Election and particularly in transmission of results, access to and scrutiny of certified copies of Forms 34A, 34B and 34C and leave to file further affidavits. The focus of this paper is on the first issue. To this end the Court granted the following orders:

> [T]he Petitioners as well as the 3rd Respondent shall be granted a read only access, which includes copying (if necessary) to –
>
> a) Information relating to the number of servers in the exclusive possession of the 1st Respondent.
>
> b) Firewalls without disclosure of the software version.
>
> c) Operating systems without releasing the software version.
>
> d) Password policy.
>
> e) Password matrix.
>
> f) System user types and levels of access.
>
> g) The IEBC Election Technology System Redundancy Plan comprising of its business continuity plan and disaster recovery plan.

[48] Ruling delivered on 26th March 2013 in *Raila Odinga V Independent Electoral and Boundaries Commission & Others* [2013] eKLR

h) Certified copies of certificates of Penetration Tests conducted on the IEBC Election Technology System prior to and during the 2017 General and Presidential Election including:

   i. Certified copies of all reports prepared pursuant to Regulation 10 of the Elections (Technology) Regulations, 2017; and
   ii. Certified copies of certificate(s) by a professional(s) prepared pursuant to Regulation 10(2) of the Elections (Technology) Regulations, 2017

i) Specific GPRS location of each KIEMS Kit used during the Presidential Election for the period between and including 5th August, 2017 and 11th August, 2017.

j) Certified list of all KIEMS Kits procured but not used and/or deployed during the Election.

k) Polling station allocation for each KIEMS Kit used during the Presidential Election.

l) Technical Partnership Agreement(s) for the IEBC Election Technology System including but not limited to:

   i. List of the technical partners;
   ii. Kind of access they had; and
   iii. List of APIs for exchange of data with the partners.

m) Log in trail of users and equipment into the IEBC Servers.

n) Log in trails of users and equipment into the KIEMS Database Management Systems.

o) Administrative access log into the IEBC public portal between 5th August 2017 to date.

p) The information listed in (m), (n) and (o) above shall be issued in soft copy to the petitioners and 3rd respondent.

q) Certified photocopies of the original Forms 34A's 34B's and 34Cs prepared at and obtained from the polling stations by Presiding Officers and used to generate the final tally of the Presidential election, and pursuant to such production leave be granted for the use of an aid or reading device to assist in distinguishing the fake forms from the genuine ones.

r) Forms 34A 34B and 34 C from all 40,800 polling stations.

s) Scanned and transmitted copies of all Forms 34A and 34B.

This was by far the most technical issue ever put forward for determination by the Courts particularly in the realm of use of technology in the elections.

5.2. Emerging judicial issues on technology

As the elections of 2017 were premised on technology, it was very difficult to be circumvented as it was core to the resolution of the dispute. In addition, the Court had very limited time as it was operating within the very narrow contours of constitutional timelines[49]. While the Supreme Court had on its own motion in the 2013 presidential petition sought to scrutinize the forms to better understand the vital details of the electoral process, and to gain impressions on the integrity thereof,[50] this time the Court was being called upon by the petitioner to directly decide a technical technology related question. In its analysis, the Court appreciated that its Presidential Elections Rules were silent on scrutiny. Nevertheless, the Supreme Court was guided by section 82 of the Elections Act as had been addressed by the Supreme Court in the 2013 presidential election petition section 4 of the Access to Information Act[51] which allows access to information in whatever form, section 27 of the IEBC Act[52] which deals with the IEBC's management of information and Regulations 15, 16, and 17 of the Elections (Technology) Regulations.

The most technical bit of this ruling was the access rights granted to the to the electoral system. It was interesting to note that within that limited duration between the argument of the application and the ruling barely two days later, the Judges had sieved through the application and narrowed down, unanimously, on which prayers to grant. The Court opted to have the access process proceed concurrently with the main hearing. In the premises, the court designated a court ICT officer from among its ICT staff and two independent IT experts appointed by the Court to supervise the more IT aspects of the access to the technology system and file a report by close of business on the next day upon which parties would be at liberty to submit on. In addition, each of the parties to the petition was entitled to have a maximum of two agents/ experts who were to comply with the directions of the ICT officer to ensure expeditious conclusion of the exercise.

This being the first time the Court had delved into such technical matters; this paper brings to the fore issues arising as it lays a basis for future engagement. At the onset it is understandable that the access to the electoral system and process had to be undertaken concurrently with the main hearing of the petition. The curious point that comes out of the ruling is whether the judges had already anticipated the application and its decision on the same and that is why it already had chosen the two IT experts and the ICT Officer. This could be so, considering that the application had been filed earlier and by the time the matter was before the judges in open court, the Judges had already applied their minds to it including the choice of IT experts. Since the Court in in control of its processes, it can be discerned that

[49] Under Article 140(2) of the Constitution, the Supreme Court should hear and determine the petition within 14 days of filing.
[50] Paragraph 169 in *Raila Odinga & 5 Others v Independent Electoral and Boundaries commission & 3 others [2013] eKLR*
[51] No.31 of 2016
[52] No.9 of 2011

the parties had no say as to who the IT experts would be. Neither the IT experts nor the ICT officer were revealed to the parties until they met at the exercise. Indeed, it was only in the full judgment delivered on 20th September 2017 about three weeks after the determination[53] that the names of the Court appointed IT experts were revealed as Professor Joseph Sevilla and Professor Elijah Omwenga, holders of PhDs on IT and lecturers in Strathmore and Kabianga Universities respectively.[54] Did this revelation of names and particulars end up serving any purpose at that point? The answer to that question is left for future deliberation in a different context.

It would have been interesting if upon citing the experts in compliance with the Court's ruling, one or all the parties had an objection as to the involvement of either one or both experts and how that could have unravelled especially in such a highly charged political atmosphere. This is so because in highly specialized fields, experts are consulted including by Government bodies or litigants and the pool of experts may be limited or they turned out to be relatives of one of the litigants' witnesses or their respective experts. It can only have been sheer luck resulting to a huge sigh of relief when it turned out that Prof. Elijah Omwenga, the Court appointed IT expert was not related or affiliated to a Mr. Bryan Gichana Omwenga, a technology advisor employed by the Jubilee Party.[55] Besides, during such moments, any more opportunity to derail the process could not be ruled out and objecting to the appointment of the specific IT experts would be a moment. Again, were they the best choice of experts who understood the nature and scope of issues before them?

Another issue that arose is whether the route opted by the Court to have concurrent processes create a possibility of disconnect? It later emerged when the report was filed, and parties submitted on it in Court that there were contests as to the extent of compliance with the Court orders. This is because neither the judges nor the counsels who had proceeded with the hearing and not with the IT experts were in a position to tell what had happened during the access sessions. Moreover, no parameters as to the nature and extent of supervision had been set for the IT experts and the ICT officer noting that these persons had no prior formal engagement as judicial officers. It was baptism by fire with the responsibility left to them to determine how active or passive role they were to take in complying with the Court order. They were just Could this also amount to delegating judicial duties to an unnamed ICT officer and IT experts. This is juxtaposed with the order directing the Registrar of the Court assisted by any such Judicial Officers and staff to oversee the scrutiny of the forms.

The last issue that this paper raises is whether the unprecedented move by the Court was the correct one. Would it have made any difference if the IT experts steered clear of the litigation and only remain expert witnesses, but again would the other litigants want to challenge their opinion and cross examine the expert witnesses and if so where that would leave the whole process. The overreaching aspect of this analysis is the suitability of the persons that the Court sought to rely upon for this herculean task. The Court may have been satisfied as to their ability to understand the electoral infrastructure subject to the litigation.

[53] Delivered on 1st September 2017
[54] Paragraph 277 of the full judgment
[55] As described at paragraph 124 of the full judgment

5.3. Implications of this approach by the Supreme Court

In the end, the Supreme Court ended up nullifying the election of the president by a decision of the majority.[56] The extent to which the technology question contributed to that decision remains arguable but it sure did contribute. The Court stated:

> [277] Of further note is that IEBC strenuously opposed the petitioners' application for access to its servers, claiming that such access would compromise the security of the data in those servers. After considering the application, we overruled that objection and partly allowed the application. Though we did not therefore accept IEBC's said claim of compromising the security of its servers, considering the fact that having spent billions of taxpayers' money IEBC should have set a robust backup system, nevertheless to assuage those fears, we granted the petitioners a "read only access" which included copying where the petitioners so wished. The report from the Court appointed IT experts, Professor Joseph Sevilla and Professor Elijah Omwenga, holders of PhDs on IT and lecturers in Strathmore and Kabianga Universities respectively, shows clear reluctance on the part of IEBC to fully comply with this Court's Order of 28th August, 2017 to provide the information requested.

The merits of the overall decision of the Supreme Court are beyond the scope of this paper. The decision however meant that there was to be a repeat of the presidential election within 60 days of the Court's judgment as contemplated under the Constitution.[57]

Following the repeat election, further petitions challenging the said election were filed[58]. The gist of the petitions focused on whether there was the need for fresh nomination, whether the withdrawal of the contestant who had come second in the annulled election, the abstention or boycott of voting in some region violence and use of state machinery vitiated the repeat election. On technology, the 2nd and 3rd petitioners pleaded *inter alia*, that the Elections Laws (Amendments) Bill, 2017 was intended to diminish the role of technology in elections, open election results to manipulation, and signal to voters that it would not be possible to successfully challenge the results of the fresh Presidential election, even if the same were to be unconstitutional, unlawful or irregular. They stated that the said Bill has since become law, with the overt approval of the 3rd respondent, and has been gazetted[59] and sought the court's determination as to which law was applicable to the repeat election and the validity of the said amendments.[60] The Court found that these amendments introduced subsequent to the annulment were not applicable to the repeat elections. The repeat elections were unanimously upheld, and the merits of the said decision are beyond the scope of this paper.

---

[56] 4 out of 6 Judges of the Supreme Court found in favour of nullifying the elections of the president.
[57] Article 140(3) of the Constitution
[58] On 6th November 2017, two petitions were filed challenging that election: *Petition No. 2 of 2017* by Mr. John Harun Mwau and *Petition No. 4 of 2017* by Mr. Njonjo Mue together with Mr. Khelef Khalifa
[59] As Election Laws (Amendments) Act, Number 34 of 2017
[60] Paragraph 377 of the Judgment

On another front, the decisions of the Supreme Court as the apex court are binding on the Courts below though not binding on the supreme court itself.[61] This means that unless the Supreme Court changes this position in a subsequent matter, the approach adopted binds other courts. It was no wonder therefore that the High Court which had the original jurisdiction to hear and determine election petitions issued similar orders designating the Deputy Registrars to oversee the scrutiny efforts. Indeed, in *Cyprian Awiti & another v Independent Electoral and Boundaries Commission & 2 others* [2019][62] which had reached the Supreme Court, the learned judges remarked that:

> [79] It is clear to us that the core question in the appeal is: what is the relevance of the scrutiny report of 24 January 2018 to the proper disposal of the election dispute?

The appellant had argued as part of its grounds of appeal to the Supreme Court that the Court of Appeal erred in law, in violation of Articles 38, 81, 86, 87 and 100 of the Constitution, by failing to consider the Judiciary's Deputy Registrar's scrutiny report of 24 January 2018.

Some petitioners in subsequent petition went to the extreme by automatically seeking the invalidation of results on the sole ground that the IEBC had conducted elections which had been annulled by the Supreme Court and that there was no need for further interrogation. While it may be argued that this decision, having been made in an election dispute only binds the superior courts in election matters, there is a possibility that the principles nay be extended to other type of disputes where the Court may decide to direct experts and its staff to supervise certain aspects of the proceedings before the Courts.

CONCLUSION AND RECOMMENDATIONS

While the Covid-19 pandemic has shifted focus on how judges should adapt to technology in the course of their day to day work in embracing virtual hearings, online filing and judgments being remitted virtually, the focus of this paper is on the actual adjudication of the technology related disputes in such a high voltage environment, such as the highly political presidential elections where the winner takes all and the Court has to adhere to a constitutional timeline. The issues raised are by no means all and this paper merely acts as a rallying call for future interrogation of the issues noted. The solution can only be as a result of considered positions.

The Court should be lauded for taking a brave step under the circumstances and not shying away from resolving a technical question. Perhaps the Court can consider under its Presidential Elections Rules to come up with a firm way of dealing with such disputes including use of IT experts should it come to that.

While technology was presumed to be the panacea of electoral malpractice, it seems that the malpractice has merely elevated to the digital sphere. The problems surrounding the electoral process seem to transcend the laws into more of mistrust on the part of the electoral management body aided by the state machinery

[61] Article 163(6) of the Constitution
[62] [2019] eKLR

commonly referred to as the *deep state*. It is no surprise that the proposed Election Law Amendments under the BBI initiatives seek to address the personnel question more than the technology deployed. The BBI may be touted as the solution to all our problems, but it must be accompanied by genuine desire by those involved in management of elections to adhere to the Constitution and the law independently to weed out the perception of their being compromised.

Finally, like any other initiatives introduced, they must be accompanied by sufficient capacity building. This is by making the Judiciary as well as the Advocates who end up litigating on these issues on their client(s') behalf before courts to create a synergy between the technology questions in practice and in the law.

READYING FOR THE SINGULARITY: FRANCES HAUGEN'S TESTIMONY AND FACEBOOK AS A CASE STUDY IN THE EMERGING METAVERSE PROJECT

Joshua Kingdom[*]

ABSTRACT

We can summarize singularity as a point in the future when Artificial Intelligence (AI) finally supersedes human intelligence. While this might sound bizarre for some, this article addresses what the author views as evidence for the possibility of this eventuality. Persistently, there is a bridge between human beings and technological inventions. Examples in the recent past are avatars in games that embody human beings in real life. Others include lifelike human sex dolls, driverless cars, AI powered chat agents, to mention but a few.

This work asserts that this bracket embodies the Metaverse, a multi-billion project brought to light, in part, by Facebook's Mark Zuckerberg. In its promotion, Tech-guru promises that Meta has the potential to alter our online interactions as it seeks to build a world of its own, almost independent of anything else. Mark Zuckerberg promises that principles only formerly applied in offline arrangements will come to the fore of the Internet under Metaverse. If successful, this will alter our understanding of life and ourselves forever, making this a perfect case study.

In that pursuit, this article is broken down into four main parts: the singularity; the Metaverse; Frances Haugen's testimony; and the eminent challenges that the advent of this project is likely to pose to regulators.

[*] LLB (Cand.), *Makerere University*. This article is written with thanks to Alyce Namale, my friend and colleague, whose continuous encouragement kept me on course in my preparation.

INTRODUCTION

Technology has a complex history. However, a flashback to the late 90's would show a dramatic change in events from what was known in the past. Previously, taking time to advance (especially in the pre-industrial age), what we can now do and not do with machines is changing at a pace so fast that no one can claim to fully explain these developments. Several traits are consistent with this period, one of which this article focuses on is singularity.

We can summarize singularity as a point in the future when artificial intelligence finally supersedes human intelligence. While this might sound bizarre to some, this article addresses what the author views as evidence for the possibility of this eventuality. Persistently, there is a bridge between human beings and technological inventions. Examples in the recent past are avatars in games that embody human beings in real life. Other examples include driverless cars and erotic toys.

This work asserts that this bracket includes, among others, Metaverse. A multi-billion project brought to light, in part, by Facebook's Mark Zuckerberg. In its promotion, the tech-guru promises that the Metaverse has the potential to alter our online interactions, as it seeks to build a world of its own almost independent of anything else. We expect principles only formerly applied in offline arrangements to pioneer under this project, and so without a doubt, if successful, this will alter our understanding of life – let alone ourselves – forever, which makes it a perfect case study.

In this attempt, this article broadly handles four key areas: singularity, the Metaverse, Frances Haugen's testimony, and the eminent challenges that the advent of this project is likely to pose to regulators.

Under the singularity and the Metaverse, the article adopts a descriptive tone, first highlighting what each of the two stands for and then arguing for why it is the case that we are already *en route* for both. This work views the Metaverse as an event in the awaiting eventuality of the singularity, that is, the biggest development in that regard. Cognizant of the fact that this link may not be fully appreciated, the writer goes at length to raise different reasons in defence of this theory.

Finally, the last two sections aim to help the reader understand the challenges that the project possesses in policymaking with the aid of Frances Haugen's account. Ms. Haugen is an American whistle-blower who, last year, revealed dark secrets about the operations of Facebook. In this, I hope to make the case that even in its rebranding to Meta, Facebook remains a devil that we now know and should accordingly be able to better equip ourselves to restrain her deeds whenever she crosses the line as well as the deeds of companies in the same trade.

From this and other analogous cases, the article deduces the challenges likely to be faced by regulators in the era of the Metaverse. The idea is that once appreciated, governments and other stakeholders can prepare to quell them while maintaining the incredible capacity that the Metaverse promises to add to the Internet.

2. THE SINGULARITY

Often, when topics such as the present one are discussed, those reading or listening tend to think that the author or speaker knows exactly how it is that the future will look like. From where I stand, I would argue that no one really knows how it is that the years to come will unfold. However, this is no less reason for one to think critically about the future. If anything, it is salient that we examine the most plausible hypotheses in that regard and equip ourselves to face them when time comes. Along this line, one of the most anticipated eventualities is that which has come to be known as *singularity.*[1]

First coined by the mathematician Vernor Vinge, the term is understood to mean a period in time when artificial intelligence (AI) grows exponentially and then in an explosion, supersedes human knowledge.[2]

Thinkers argue that it would be impossible for human beings to perceive the environment around them using their natural cognitive senses. To be able to keep-up then, humans would have to adapt to the ways of the machine, also understood as the age of the Transcendent Man in futuristic language.[3] In other words, there will be no separation between that which is human at that point and that which is born of technology.

This is the final step of this course. There are several other developments in the way that one can think about. Consider prosthetic enhancements such as. This helps individuals accomplish tasks that they would otherwise not manage.[4]

The fact that these modalities appear in early stages may mean that there exist key distinguishing features between them and the singularity, say the fact that human-machine relations at the moment are more with the outer-body functions of different organs, while the singularity is more about neuroscience. However, this does not make the innovations less significant. On this scale, the Metaverse can be viewed as occupying the middle, considering that it embodies properties on either side of the spectrum.

In anticipation of singularity, there has been a deep divide between writers, movie directors, etc. about the exact form it will take, perhaps unsurprisingly. A significant amount of material churned out thus adopts a dystopian staging of this

[1] Many notions have been elucidated here. Consider for instance the idea of exponentially increasing our life expectancy as human beings to say, three hundred years (Science Daily; Pathways that extend lifespan by 500 percent identified; Discovery of cellular mechanisms could open door to more effective anti-aging therapies, Available at: https://www.sciencedaily.com/releases/2020/01/200108160338.htm, last accessed on 15th-August-2022).

[2] Doug Wolens, *The Singularity: Will We Survive Our Technology*, Spring, 2016.

[3] This idea is born of the author Ray Kurzweil in a movie under the same title espoused a belief that as a species we are gradually coming closer to a point in which machines merge with people to give rise to an entirely new, "Transcendent Man" (Transcendent Man Definition, available at; www.encyclo.co.uk, last accessed on 9th-September-2022).

[4] This is the kind of technology that enables Lord Vader to survive and continue to fight in the movie Star Wars after a fight with his master Obi-Wan Kenobi which sees him lose all his limbs, a movie by Lucasfilm Ltd. In real life, this technology has been hugely embraced at the Paralympics (Innovative prostheses positively change the Paralympics, Available at www.wipo.int, last accessed on 9th-September-2022)

coming time, that is, make the world as it is today more admirable. On the other hand, an equally significant number of creatives have painted the opposite stance, instead of eutopia. While Adolf Hauxley's *Brave New World* for example, tells the story of a factory that deals with hatching babies despite the fact that its owner has a child of his own acquired through sex, Neal Stephenson is more optimistic about *Snow Crash*,[5] when creating a deadly virus, the kind that appears in the movie Matrix_[6] he creates the *numb-shum* built by *Enki* to counter the crisis.

Thus, singularity is a double-aged sword. It can at once be a period of tremendous thriving – talk about poverty eradication, elimination of all forms of disease, etc – yet it could also be a stage where human beings are completely wiped away from the face of the earth through all sorts of causes, such as the arms race. One then would see here why it is the case that enough attention ought to be dedicated to this event.

What makes this point more important is the sheer amount of progress achieved in the field of artificial intelligence (AI). IBM's Watson can comb through millions of publications every year as opposed to an average scientist who reads up to only 300 papers.[7] Similarly, AI's promise to reform transport, as we know, has begun to take shape. In Japan, for instance, deep learning[8] has enabled the government to develop technology that monitors thousands of railway track kilometres.[9] Comparatively, this system is more efficient for human effort and is often susceptible to numerous fallibilities. Add to *Tesla*'s driverless cars and see what picture you have.[10]

Even if one considers the singularity theory to be misled, at least it is not in dispute that technology is increasingly defining human relations to extents that are getting out of reach for individual decision making. Note, for example, that while two people may equally have accounts on Twitter, there will always be variation in what it is that is trending on their timelines. It is not surprising that such persons have different understandings of life. The same can go for the news we watch, the items we purchase (probably motivated by targeted advertising) to mention, but a few more areas.

Critics could argue that computers are unable to replicate features of the mind

[5] Published in 1992, Snow Crash is set at a time following an economic crisis that renders the institution of the state toothless. Much of what is conventionally federal has been overridden by private entities and entrepreneurs. Even security! In this state of chaos unfolds a story of a genuine desire to grow self and safeguard loved ones in the character of Hiro even when faced with odds of selfish yet sophisticated beings. In the end Hiro wins.

[6] A film by Warner Bros, Village Roadshow Pictures, Groucho II Film Partnership and Silver Pictures.

[7] Laura Geggel; Forget Jeopardy: 5 Abilities That Make IBM's Watson Amazing, Available at; https://www.livescience.com/50479-5-ibm-watson-facts.html, last accessed on 15th-August-2022).

[8] Deep learning refers to a tool where computers are exposed to very high volumes of data from which they can deduce certain patterns about how a particular area of life operates. United Kingdom's *DeepMind* Has demonstrated how algorithms could learn to play video games at an expert level through this process.

[9] Law & Technology: Risks and Opportunities from the Tectonic Forces at Work, Available at https://www.whitecase.com/insight-our-thinking/law-technology-risks-and-opportunities-tectonic-forces-work, last accessed on 15th-August-2022).

[10] Faiz Siddiqui; Tesla floats fully self-driving cars as soon as this year. Many are worried about what that will unleash, Available at https://www.washingtonpost.com/technology/2019/07/17/tesla-floats-fully-self-driving-cars-soon-this-year-many-are-worried-about-what-that-will-unleash/, last accessed on 15th-August-2022).

such as consciousness, which may be true, at least for the moment. Be that as it may though, the more important question is whether singularity would require that those features are discovered first (this is not to say that they cannot but that is a conversation for another day).

3. THE METAVERSE

While the reasoning mentioned above can be understood as characterizing singularity as relatable to AI more than anything, there are features that are deserving of similar appreciation, one of which is connectivity. For human beings to adopt technology at a rate that would lead them into a singularity, there is something highly attractive about it that makes interacting, communication, and other activities of day-to-day life more enjoyable.

Any emerging technology that realizes this objective should be viewed as one with the potential to be the next in the line of many that will eventually lead to the ultimate connection, that is, singularity. Presently, one may argue that social media platforms like Twitter, TikTok, and Instagram stand out as being at the heart of this form of business.[11] However, the future supersedes the reach of these innovations. This is where the verse comes.

3.1. Background and How it Works

While the term has been popularized by Facebook's move to rebrand into meta,[12] it has long been in existence. To appreciate the impact that this invention is likely to have, it is important that they understand its roots first. The use of "Metaverse" in this article thus, is not restricted to the project being run by Meta but rather the broad sense in which it has come to be known in technology and literature.

Jean Baudrillard argues that there are three ways in which to understand this simulation: the first, second, and third simulacrum. [13] In the first category, reality is clearly separable from what is imaginary, and as stages advance, the two concepts continue to be blurred. An example in the first bracket is the painting of a person, followed by a photograph in the second case.

The third stage comes to the minds of many when one mentions the word "Metaverse'." Kashif Laeeq defines it as "a simulated digital environment that combines augmented reality, virtual reality, blockchain, and social media principles."[14] The initial idea was that an individual seeking to experience this

[11] One will remember here the bitter row that former United States had over TikTok arguing that it ought to be banned (Gray, Joanne Elizabeth (2021): The geopolitics of "platforms": The TikTok challenge, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 2, pp. 1-26).

[12] Mark Zuckerberg's video on the topic was viewed over six million times (The Metaverse and How We'll Build It Together -- Connect 2021, Available at: https://youtu.be/Uvufun6xer8, last accessed on 15th-August-2022.

[13] Urška Podmenik; Neal Stephenson: Snow Crash, University of Ljubljana Faculty of Arts Department of English. Ljubljana, March 2010.

[14] Kashif Laeeq; Metaverse: Why, How and What, Available at: https://www.researchgate.net/publication/358505001, last accessed on 30th-July-2022).

realm would do so through a terminal, though the way it has played out is that a user will wear Google and earphones and through them he/she can share an experience with 3D representations of persons (also known as avatars) elsewhere. This experience is enabled by lasers pointed to the user's eyeballs.[15]

There are several forms of avatars. From robots to wild animals to creations that a person can build from scratch, one has several choices from which to present themselves. The same applies to items formerly present in the real world, such as clothes and hangouts. For any of the specifications mentioned, a Metaverse subscriber must meet the sum of the money that goes to developers within the Metaverse. Similarly, one may buy a private space and ask that only they can access it and may be invited guests.

The potential here is incredible, as opportunities will be divided evenly across the world, considering that the Metaverse realizes attributes of physical engagements, yet eliminating their necessity. Persons with disabilities are an example of a person who will have a niche here as they can and cannot extend beyond the bounds of their physical bodies. Indeed, Neal's Snow Crash gives *Ng* a second chance to walk when he purchases a vehicle tailored to his disability, something that was not possible for him in the real world.[16] This is also related to the case of Zuckerberg in the recent past.[17]

As argued for under singularity, not everyone is optimistic. The opening statement to Steven Spielberg's *Ready Player One* tells us all.[18] Talking about the OASIS_ the equivalent of the Metaverse in the movie, Wade, who is the protagonist, has this to say; "…people have long stopped trying to fix problems and just [try] to outlive them."[19] What remains clear in both these schools of thought is that whatever happens in the alternative reality has implications for those in real life.

An example of this aspect in Spielberg's movie is the fact that Wade's family is attacked and killed by agents of a corporation that views a victory for the protagonist in the OASIS as a threat to the fortune it possesses.

3.2. The Potential

To date, the ideas suggested may sound speculative or idealistic. That is not the case, and considering that I intend that the reader appreciates the veracity of what underpins the Metaverse, it is salient that we examine this notion in more depth. It is this that we will address next. Several factors are addressed below the summation of, which is the fact that the Metaverse is not out of reach of what is

[15] Trapped in the Metaverse: Here's What 24 Hours in VR Feels like, Available at: https://youtu.be/rtLTZUaMSDQ, last accessed on 5th-August-2022).
[16] Neal Stephenson; Snow Crash, Bantam Books, 1992
[17] Supra Note 10
[18] Set in 2045, Ready player one introduces a place everything poor that there is nothing to hope for but one big oasis where everyone plays games and creates all sorts of fantasies as an escape. Wade Watts one of the biggest gamers joins everybody else in the virtual pleasure and occasionally participates in a hunt to inherit hidden treasure by the originator of the oasis John Hughes. And more because of luck than expertise, he indeed lands on the secret keys leading him to inherit a fortune he couldn't comprehend till then.
[19] Valentina Romanzi; Levels of Reality in Steven Spielberg's Ready Player One: Utopia, Dystopia, and Retrotopia, University of Bergamo.

practically possible.

3.3. The Involvement of Meta

The first thing to be said is the interest that Facebook – now Meta – developed in this project. The company already boosts over five billion followers if added together with its sister companies, WhatsApp and Instagram, making it the largest social media company worldwide.[20] This means that the company is best placed to know the intricate dynamics of online personal interactions, considering the sheer amounts of data that they have about their subscribers.[21] It is this information that is needed for one intending to build the next level of reality, as already described.

Meta's following equally makes it easy for people to transition from social media as we know it into the Metaverse. One can relate this to the way people upgrade apps on a play store. The individual doing an update does not perceive their action as doing something entirely new, but rather makes better an experience that they already know about. This is a significant aspect because persons in such positions are bound to trust the platform based on their past experiences, and it is this that determines the percentage of persons who eventually join the Metaverse, the frequency with which those that join will use it, and the amount of personal information that they will be willing to share.

Suffice to say, Facebook, as an establishment, already has huge chunks of investments that enable it to easily raise the capital necessary to do the Metaverse flagship. Fully realizing the Metaverse is a very costly venture.[22] This means that the technology needed to run is still in its infancy, and so a lot must be spent on experimenting with ideas, many of which may never materialize.[23]

It is equally the case that no company can build this new cyber world single-handedly, necessitating partnerships. While Meta is, for the most part, purely a web run company, for example, the Metaverse goes beyond that. It requires the aid of hardware gadgets, such as earphones. Before businesses with the potential to deal with such products may come in, however, they must ascertain that such a venture is worth pursuing, even in its novelty. Knowing that one is dealing with a company that has proven itself over time would be essential in bringing more players on board.[24]

---

[20] We can be sure to count on Meta's interest since its proprietors knows that interaction as we have known it i.e., texting and voice-notes will soon be a thing of the past and as such there is need for them to stay relevant.

[21] To understand best the impact of Facebook, one needs to appreciate the fact that it has led to overturning of governments (see; Iliana Hagenah; How the Women-Only Facebook Group Minbar-Shat Helped Overthrow the Sudanese Government, Available at: https://www.elle.com/culture/career-politics/a29355590/minbar-shat-facebook-sudan-revolution/, last accessed on 15th-August-2022).

[22] It is estimated that the market value of the metaverse stands at USD $7 billion (Z Allam; The Metaverse as a Virtual Form of Smart Cities, Available at: https://www.mdpi.com, last accessed on 15th-August-2022).

[23] Funding is probably the single most factor that has kept the world from some of the best inventions ever made (project Ligo cost about US$395 million back in 1994).

[24] Mark Zuckerberg agrees that the metaverse must be a concerted effort. In his words, he says; 'A true metaverse means taking your "Roblox" personalized avatar and bringing it into…Meta's Horizon VR platform, or "Minecraft," or "Fortnite," or into a hypothetical Netflix virtual theatre event online.' (Gene Park; Zuckerberg's Meta promises a 'future' these video games delivered years

The success of Meta in its earlier forms is also relevant because it has brought its founder into the spotlight, where many look at him as among the top people who best understand technology in our day and age. Indeed, Mark Zuckerberg utilized this advantage to pitch the new project.[25] Another person would need to first gather traction, which is difficult to work around. Indeed, the talk about an alternative reality has always been around yet it did not pick up in any of these cases until the Meta CEO re-introduced it.

Of course, we must be alive to the fact that the magnitude of Meta does not mean that they cannot invest in projects only for them to fail.[26] My point here is to say that regardless of the eventuality of such projects, the points stated already make each such venture significantly different from those picked on by persons that the public may not know.

3.4. The Emergence of Accompanying Technology

The current age has come with tremendous innovations. Many previously unimaginable tools are currently a reality. This is true for projects unrelated to the Metaverse,[27] as it is with those related to it. Consider the advent of blockchain technology, for instance, which has enabled the issuance of credible money perfect to replace central banks' issued currency and doing so at a much cheaper cost.[28] Blockchain has equally enabled inventions, such as non-fungible tokens, that enable the replication of real-life experiences, such as personal property ownership in the virtual world.[29] It is important to note that such items, such as private homes and clothes, cannot be fabricated by anyone else once purchased, and as such, the possessor would have exclusive ownership of them.

Various industries have long employed different aspects of their trade that will be employed at this new level. During this time, they have had time to develop these functions to levels that can match those which will be employed in Metaverse. A good example is the gaming industry, which has all the avatars used.[30]

This means that Meta and other inventors do not need to start from scratch, as they build this project. This also means that there will be a reduced time between when this project was born and when it was completely operational. Moreover, the fact that these companies have succeeded in what they do is an indicator of the

---

ago, Available at: https://www.washingtonpost.com/video-games/2021/10/29/facebook-meta-rebrand-metaverse-video-games/, last accessed on 15th-August-2022).

[25] Supra Note 10.

[26] The crypto-currency project is a good one here (Facebook Libra: the inside story of how the company's cryptocurrency dream died, Available at: https://www.ft.com/content/a88fb591-72d5-4b6b-bb5d-223adfb893f3, last accessed on 15th-August-2022.

[27] Supra Note 20

[28] Ntamugabumwe Victor and Joshua Kingdom (2021), "The Legal Risks of Cryptocurrency on State Sovereignty; A Case Study of Uganda" Volume 18 Issue 3, Makerere Law Journal pp 118-152.

[29] How the Metaverse Will Design Our Cities, Available at https://www.propmodo.com/how-the-metaverse-will-design-our-cities/, last accessed on 15th-August-2022).

[30] Roblox is one of them.

market for their products.[31] As already explained with the persons using applications under Meta, it can still be argued that this market can be tapped into once the Metaverse fully rolls out.

The presence of other players equally helps to divide costs. This is important considering that a project of this magnitude requires massive investment in sums that might not be attained by one company on its own. [32] Similarly, this set of events enables specialization, which allows for efficiency. Thus, the final product is more likely to be attractive and more people will be willing to use it.

3.5. COVID-19

Many things can be said about COVID-19 and one of them is how reliant people became on technology. This was due to the measures adopted by governments, such as lockdowns that had the effect of separating individuals, even when they needed to be together, say workmates.[33] This meant that there was a spiral in the usage of platforms such as Zoom,[34] Microsoft Teams, and Google Meet as people shifted from physical engagements to online setups.

This had the effect of introducing the world to an atmosphere that, though previously in existence, did not feel the necessity to relate with it. These applications have demonstrated much capacity to the extent that many have continued to employ them even when the previous restrictions have been lifted. This is an opportunity that proponents of the Metaverse can benefit from if harnessed well, as this project aims to make such experiences even better.

Had that not been the case, this technology would have taken a natural course before booming.[35] Scholars have described the notion here to reflect a pattern of human society; that is, every pandemic alters our interactions in ways previously unknown to us.[36]

3.6. Promising Results

Indeed, one can already see that progress is being made with the Metaverse to the realization of the already laid hypotheses. Consider, for instance, the fact that both Gucci and Balenciaga collaborated with developers Roblox and Epic Games

[31]The global gaming market is set to reach $256.97 billion by 2025 (Teodora Dobrilova; How Much Is the Gaming Industry Worth in 2022? [+25 Powerful Stats], Available at: https://techjury.net/blog/gaming-industry-worth/#gref, last accessed on 15th-August-2022).

[32] Supra Note 19.

[33] In the case of Uganda, the president issued measures including lockdowns in several of his addresses (address - Embassy of Japan in Uganda, Available at; https://www.ug.emb-japan.go.jp, last accessed on 15th-August-2022).

[34] While zoom hosted 200 million meetings throughout 2014, in April 2020 it announced that it would host 300 million meetings in a single day (Brian Dean; Zoom User Stats: How Many People Use Zoom in 2022?; Available at https://backlinko.com/zoom-users, last accessed on 15th-August-2022).

[35] Natural growth of projects often takes more time than that. Facebook for instance was started in 2004 until its take-off around 2010 (Mark Zuckerberg (Facebook)- From Harvard to the Facebook, Available at; https://castbox.fm/x/id65, last accessed on 15th-August-2022).

[36] Yuval Noah; Sapiens: A Brief History of Humankind, Dvir Publishing House Ltd 2011

to recreate their merchandise in a virtual form.[37] Similarly, Roblox recently hosted a concert in Fortnite that was attended by over 60 million people. The concert also enabled functions not possible to replicate in the real world to the amusement of the audience, for example, beat drops throwing everyone in the air.[38]

This is not to say that there were no challenges in this system. For instance, all companies engaged in building platforms in virtual reality will need to synchronize their operations such that an individual can own a single avatar across several platforms. This requires a degree of standardization. Compared to the huddles already overcome, however, one can confidently assert that the challenges in question are less veritable. From the innovator's perspective.

4. FRANCES HAUGEN'S TESTIMONY

Notwithstanding the potential explored above, an investment of a magnitude similar to that described deserves a cautious approach. This is something that has been highlighted previously.[39] Perhaps there is no event in the recent past that has helped elaborate this fact, like the decision by Frances Haugen, a former employee of Facebook working in the Civic Integrity Department to publicly rebuke her former company over what according to her are multiple business irregularities.

First appearing as internal documents leaked to the media, Ms. Haugen's testimony disclosed disturbing truths regarding how Facebook worked.[40] From the reporting, subscribers would come to learn that the algorithms employed by Facebook unfairly targeted young people, and that the company had made a significant contribution to the organization of the January 6th match to Capitol Hill, an event that tainted democracy in the United States in bad light.[41]

The far-reaching impact of these claims would even garner more credibility when the formerly unknown whistle-blower eventually put a name and face to them. This saw her interview with a different press and her eventual appearance before the senate Subcommittee on Consumer Protection, Product Safety, and Data Security.[42] While there, Ms. Haugen elucidated her claims, arguing that Facebook recommended foods that made children likely to become obese. She equally argued that platforms such as Instagram were far worse off when it came to the mental health of minors compared to say TikTok, since while the latter app mainly hosts individuals sharing funny videos, Instagram is mainly about teenagers sharing their physical looks and comparing themselves with others.

As if this was not enough, Ms. Haugen revealed that the company was perfectly aware of these issues (in fact, everything leaked was part of Facebook's internal

[37] Supra Note 12.
[38] Supra Note 12.
[39] Stephen Hawking et al., Transcending Complacency on Super-intelligent Machines, HUFFINGTON POST (Apr. 19, 2014)
[40] Inside Frances Haugen's Decision to Take on Facebook, Available at: https://time.com/6121931/frances-haugen-facebook-whistleblower-profile/, last accessed on 15th-August-2022).
[41] Why You Should Be Worried About Facebook's Metaverse, Available at; https://youtu.be/bolyiGMcjBs, last accessed on 15th-August-2022).
[42] Facebook Whistleblower Frances Haugen testifies before Senate, Available at: https://youyu.be/GOnpVQnv5Cw, last accessed on 15th-August-2022).

research) and, therefore, that it had just not acted on them.[43] Indeed, there is a clear lack of clarity on such issues in Facebook's responses to these allegations. For instance, Mr. Zuckerberg resorted to rhetorical language, asking why a company disinterested in the welfare of its users would carry out research, as cited by Ms. Haugen.[44] The follow-up question here is why the company would not act even on learning such disturbing facts. Fortunately for Mr. Zuckerberg, there was no interviewer.

While questioning Ms. Haugen, the committee's chairman Sen. Richard Blumenthal corroborated her account, citing that his office had successfully created a fake account of a minor (below the legible of 13 years) on Facebook with relative ease.[45] The chairman would further explain that in the time following the creation of the said account, the Facebook algorithm treated the purported user to worrisome scenarios, such as recommending unhealthy foods.

In summary, the picture drawn following Ms. Haugen's statement was that of a company that was fronting profits over people. It was a bitter reminder of other previous _and perhaps less substantiated, but equally gruesome_ accusations held against Facebook. For instance, there is evidence that the platform has been employed by dictatorships to suppress minorities, as in the case of the Rohingya in Myanmar.[46]

In considering this, one must also consider that the testimony in question is from just one employee of several thousand that the company employs across the world. It is evidently possible that there is a lot more concern about Facebook's behaviour that we are yet to learn. It is also the case that Facebook is a single company of many that occupy a similar position and therefore susceptible to acting in precisely the same way if not worse. Indeed, Ms. Haugen mentioned that she had been approached by a number of her former workmates thanking her for being courageous, where they on their own could not.

5. REGULATING THE METAVERSE

Ms. Haugen's testimony pointed to policymakers, and anyone interested in the direction of the regulation. From the facts disclosed, it is clear that it is not possible for Facebook to self-regulate entirely because there seems to be no direct incentive. In anticipating the Metaverse, the author's argument is that regulators should pick on from these pointers. The justification here is that which has been explained already, i.e., both the Metaverse and Facebook are platforms that people employ in their day-to-day interactions the only difference being that they operate at different levels.

[43] Some scholars have in fact argued that the whole meta project is meant to overshadow the bad publicity that befell Facebook in the awake of Frances Haugen's testimony (Supra Note 38)

[44] Libbey Cathey; Zuckerberg breaks silence, denies Facebook whistle-blower's claims; Available at: https://abcnews.go.com/Politics/mark-zuckerberg-breaks-silence-denies-facebook-whistleblowers-claims/story?id=80432492, last accessed on 15th-August-2022).

[45] Supra Note 39.

[46] Rohingya sue Facebook for £150bn over Myanmar genocide, Available at: https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence, last accessed on 15th-August-2022).

The Metaverse would thus need even more attention considering that it involves a more wholesome experience, which in effect means that subscribers must give more of themselves, say, in terms of personal data.[47] It is also crucial that this conversation starts now, as opposed to later, as is always the case, that is, regulation coming way after technology has advanced.

5.1. Flaws of Legislating

The first challenge is that they are generally associated with legislation. In fact, companies involved in building the Metaverse will certainly take active steps to prevent measures geared at combating risks associated with their inventions, as companies have done before. It goes back to the conflict between profit-making and public interest. This struggle was witnessed more severely during the passage of the Children's Online Privacy Protection Act in the United States.[48] Businesses undermine the legislature by actively lobbying for measures that serve their models, ensuring that they reach the widest pool of potential subscribers.[49]

This is quite a big blow since legislation is the only legitimate way that has the potential of helping avoid the damage that market players are likely to cause to consumers.[50] Other alternatives that one can think of are rather limited in reach. A good example is consumers' individual choices. The challenge here is that individuals may not on their own be able to tap into advantages such as summoning the best experts to guide them on appropriate choices to take.

Even though it was possible, however, by reading the literature published by such persons, there are always other limiting factors. One of them is the sheer amount of time that would take, especially if understood through the lens of the volumes of laws that legislative houses have to pass in general. On the other hand, some members of the citizenry are constrained by factors such as not being literate and thus unable to dissect policies with the level of astuteness that their representatives would.[51]

---

[47] It is estimated already that computer users create 2.5 quintillion bytes of data every day. This will only grow exponentially in the era of technologies like the metaverse which require added personal information say the movement of a person's eye lashes to be able to build technology that helps improve the eye contact experience. (10 Technology Challenges (Available at: www.10%20Technology%20Challenges%20-%20SGR%20Law.htm)

[48] One of the major issues herein was the age of children to be covered by the Act, COPPA (Children's Online Privacy Protection Act), Available at: https://www.techtarget.com/searchcio/definition/COPPA-Childrens-Online-Privacy-Protection-Act, last accessed; last accessed on 15th-August-2022).

[49] Businesses inclusive of which are big-tech companies spend humongous sums of money to have leaders that represent their interests get elected. One source revealed that $10.3 billion in lobbying was spent at the federal level and across the 19 states in 2020 (Anna Massoglia and Brendan Glavin; Federal and state lobbying spending soared to $10 billion during the 2020 election cycle, but state lobbying disclosure remains limited, Available at: https://www.opensecrets.org/news/2022/03/federal-and-state-lobbying-spending-soared-to-10-billion-during-the-2020-election-cycle-but-state-lobbying-disclosure-remains-limited/, last accessed; last accessed on 15th-August-2022).

[50] One of the moments that are still revered to this day in this line is the appearance of tobacco owners in congress (Allan M. Brandt, P; Inventing Conflicts of Interest: A History of Tobacco Industry Tactics, Am J Public Health. 2012 January; 102(1): 63–71)

[51] This is particularly the case for developing countries (Derrick Wandera; New report reveals 60% primary pupils, Available at: https://www.monitor.co.ug/uganda/news/national/new-report-reveals-

That is, one perspective, however. The other is for an overzealous legislature to pass laws that are unreasonably limiting, usually owing to misjudgement and, in other instances, petty reasons such as political aligning. Here, legislators ought to realize that good laws can create or break an industry. The alternative gives rise to black markets, and transfers business to states where they can easily manipulate the legislature, all of which are effects not good for an emerging industry like the Metaverse.[52] Thus, adopted laws should look at reflecting hybrid solutions that leave room for internal measures provided that tech companies continue to be supervised by legitimate authorities.[53] An example from social media platforms as they appear today is the option that enables users to block persons with whom they are uncomfortable sharing a platform.[54]

Legislators must be proactive, vigilant, and ready to learn to combat these challenges. It is the case, for example, that technologies such as the Metaverse are only emerging at a time when the majority of them have already come of age and so one dealing with them would need to understand the complexities of the virtual world first-hand. Moreover, this is an emerging technology and there are not many precedents to benchmark on, as is usually the case with passing of laws.[55] This means that legislators should be ready to spend considerable resources and money, to say the least, to be able to arrive at responsive laws.

The two factors explained thus make lawmakers more susceptible to tricks that investors are likely to employ in a bid to satisfy their selfish interests. In the wake of Frances Haugen's testimony, Facebook and its affiliated companies went through a major outage lasting nearly six hours.[56] It is difficult to think that this was a coincidence, yet no one might ever know why it occurred.

5.2. Existing Problems Crossing over with Greater Impact

In envisaging the future of law and the Metaverse, regulators must examine existing challenges with the use of technologies. If not carefully addressed, these issues will replicate themselves even at this level with even worse ramifications.

In relation to Internet accessibility and data costs, for instance, the developed world incurs far more huddles than the developing world. [57] This is quite concerning because one would imagine that projects like Metaverse that have high

60-primary-pupils-can-t-read-3867420, last accessed; last accessed on 15th-August-2022).

[52] Thomas Sowell; Basic Economics, Basic Books, 2004

[53] Arguments on self-regulation have been mostly made by proponents of crypto currencies (Roy Keidar; Cryptocurrencies and Market Abuse Risks: It's Time for Self-Regulation, January 2018SSRN Electronic Journal)

[54] It is of course true, that at times these measures are quite limited in their implications. It isn't very likely for instance that many users read in detail terms of usage later back-off in the event that such terms contradict what it is that they can commit to.

[55] An example of these benchmarked laws is the 2019 Uganda Data Privacy Act which mostly reflects the European regime.

[56]Soo Kim; How Long Was Facebook Down and What Caused the Outage?, Available at; https://www.newsweek.com/facebook-instagram-whatsapp-downtime-outage-cause-1635530, last accessed on 15th-August-2022.

[57]Indeed, the 10 least internet penetrable countries across the world are developing nations, Countries with the lowest internet penetration rate as of April 2022, Available at; https://www.statista.com/statistics/725778/countries-with-the-lowest-internet-penetration-rate/, last accessed on 15th-August-2022.

functionalities will require more volumes of data consumption as well as a stable network. Problems such as these need to be anticipated and worked on in time if the objective of providing equal opportunities as envisaged by Metaverse developers is realized.

This is not just a problem that exists with the use of the internet. Problems in the real world can follow the same pattern.[58] This is the case because, as explained previously, the Metaverse, as opposed to other forms of interactive technologies, will adopt unprecedented levels of physical-world-like experiences, such as ownership of land, wearing clothes, etc.

A good illustration of this is discrimination, say on grounds of colour, which has been a recuring theme in the recent past.[59] Knowing that AI is dependent on human intervention, there is a looming risk of biases passing from humans to algorithms, for example, under deep learning. This would cause an even more devastating state of affairs since machines can easily be defended as uninclined to make unfair decisions because they have neither flesh nor feelings.

These disparities are likely to surface in international relations. While the developed world may be able to pass laws that are strict and can achieve the desired outcomes, it is not clear whether developing countries can do the same.[60] Countries such as China have demonstrated, for instance, that they are able to invent their own social media companies even in the absence of big global players such as Facebook.[61] However, in the case of countries like Uganda, governments have failed to effect mere bans on companies that they have issued directives against. .[62]

Other existing problems that could worsen, if not anticipated and catered for, include questions on liability in events of harm caused by subscription to and usage of a platform. It is difficult to determine whether it is the manufacturer to meet the accompanying consequences, as artificial intelligence operates somewhat autonomously.[63] In the event that liability falls on the AI, it is not clear how the victim can be compensated by a machine.

5.3. Overhauling Law as we Know it

When one thinks of regulation, they simultaneously think of law. Apart from the fact that regulatory instruments are laws, enforceability is a mechanism under the

[58] In the Snow Crash novel for instance, the existing police force is up for those that can pay them most there recreating militias that characterize quite a significant fraction of failed states.

[59] Teresa Chen; Black Lives Matter: Power, Perception, and Press (Harvard Kennedy School, Harvard University
Fall 2021).

[60] The 2019, European Union's General Data Protection Regulation for instance requires organizations in Europe that handle data from individuals in the EU to report breach incidents to regulators within 72 hours of learning such breaches. Failing to do so can attract up to 4 percent of a company's annual global revenue.

[61]As it stands, We Chat has over a billion subscribers (Global social media Statistics, Available at; https://datareportal.com/social-media-users, last accessed on 15th-August-2022).

[62]Ugandans resorted to use Virtual Private Networks (Why Ugandans are still using VPN despite restored access to social media, Available at; https://www.independent.co.ug/why-ugandans-are-still-using-vpn-despite-restored-access-to-social-media/, last accessed on 15th-August-2022).

[63] *Doe v. Uber Techs* Case No. 19-cv-03310-JSC (The case examines liability at the level of independent contractors).

judicial system. When one considers the fact that the Metaverse possesses real risk to this sector, one equally knows that the repel effect would be felt under the regulatory frameworks.

Many warnings of how it is the case that technology will dramatically redefine the legal profession have been made, yet the attributes that the Metaverse brings with it may by far supersede these predictions. While Richard Susskind, for instance, points to question-and-answer algorithms that are likely to devise legal solutions when visited via websites in *Tomorrow's Lawyer*,[64] the Metaverse has the ability to add to this capability only lawyers could previously provide, that is, a sense of interaction with another person. Adding to these attributes, such as a reduction in the costs of legal fees and convenience, many lawyers will potentially have no job.

Moreover, the Metaverse has the potential to redefine international trade. If the examples pointed out regarding the partnership between Gucci and Roblox are anything to go by, it would mean that eventually people will hardly have to import anything but for constants like food. This is notwithstanding the sheer amount of export trade in the fashion industry today.[65] As such, taxation, which is one of the major earners of revenue for governments, is likely to suffer a major blow. Prestigious institutions such as the World Bank, the World Trade Organization, and related legal regimes must restructure themselves to match new realities.[66]

The real challenge will come if, during readjustment, entrepreneurs utilize the gaps that exist at the time to expand their influence while at the same time occasioning fears associated with non-regulation. Fortunately, there is hope that lies in some of the deepest far-reaching norms of modern law that have the potential to extend into the Metaverse era. A good example of this is the notion of human rights.[67]

CONCLUSION

The case of a Metaverse is complex. Considering the different scenarios examined, it is important that regulators begin to work on measures to be adopted depending on the nature of the Metaverse project. In this way, we can buy time to alleviate the possible detriment, like the one examined in the last section of the article.

This task requires, first, that legislative bodies understand the significance of the Metaverse and, as such, do not view it as one other invention, and more importantly, appreciate the place it holds in the singularity project. It is the writer's hope that this article will invest efforts to help realize this goal.

[64]Originally published in 2013.

[65] It is for instance estimated that Italy exported clothes worth 22.35 US Dollars in 2020, Value of clothing exports from Italy 2000-2020- Statista (Available at; www.statista.com, last accessed on 9th-Sept-2022.

[66] The world trade organization as a case in point has a very elaborated process characterized by a whole set of events in history (Peter Van den Bossche and Werner Zdouc, *The Law and Policy of the World Trade Organization*, Cambridge University Press, United Kingdom).
Text, Cases and Materials

[67] Article 1 of the Universal Declaration of Human Rights declares that all human beings are born equal with the same rights.

This understanding will help develop an approach that is wholesome in terms of the stakeholders involved, the resources mobilized, and the degree of scrutiny met on the different players in the industry. In this way, we can guarantee that there will be gains from the positives that the Metaverse will bring with it while simultaneously undermining the damage it can potentially cause.

To understand this better, concerned persons should look no further than Frances Haugen's testimony to congress.

NO TO BIG BROTHER: THE LEGALITY AND IMPLICATIONS OF MASS DIGITAL SURVEILLANCE IN UGANDA

Nasser Konde*

ABSTRACT

The Government of Uganda intends to carry out mass digital surveillance on Ugandans in the form of full-time tracking of the movement of all motor vehicles, motorcycles, and boats. The government contends that this tracking is aimed at curbing crime following numerous high-profile assassinations and the assassination attempts of key public figures and government officials. This paper interrogates the legality and implications of mass digital surveillance in light of the right to privacy, which is guaranteed by international and regional human rights instruments, the 1995 Constitution, the Data Protection and Privacy Act 2019, and the Data Protection and Privacy Regulations 2021.

*BIT (MUK), LLB (MUK), CCNA.

INTRODUCTION

Digital technologies have revolutionized our day-to-day lives, creating minutely detailed records. The Ugandan government has shown keen interest in acquiring this data and using it for unknown purposes, although it claims that it is going to use it for national security purposes.[1] On Friday 23 July 2021, the Government of Uganda entered into an agreement with Joint Stock Global Security Limited, a Russian based company to install tracking devices in all motor vehicles, motor cycles and boats in the country to track them in real time.[2]

The proposed mass digital surveillance dubbed Intelligent Transport Monitoring System (ITMS) according to the Minster of Security Maj Gen (Rtd) Jim Muhwezi will be used to determine which vehicles were in what place once there was a security situation. With this system in place, the government and implementing partners always have access to the location of any automobile.

To implement the system, all vehicles are re-registered and issued with a new number of plates embedded with a tracking device.[3] According to the Government, this measure is meant to curb crime and the increasing targets of high-profile government officials and private individuals in the country by assassins. This came after the assignation attempt on General Katumba Wamala, then Minister of State for Works and Transport, which led to the death of his daughter. [4] For some Ugandans, the Government's intention to curb criminality and promote national security by tracking in real-time motor vehicles, motorcycles, and boats is a guise to legitimize the real-time mass digital surveillance of Ugandans, especially those opposed to the government and opposition politicians. [5]

One cannot blame Ugandans for being cynical about their government given the global trends regarding the misuse of surveillance and digital surveillance powers, particularly by governments and regimes, to keep an eye on dissidents, critics, those opposed to the regime, and opposition politicians. This begs the question of why the government entered a contract with a foreign private company to carry out real-time mass tracking when it could have done so by itself and if not capable, built the capacity to do so if its intention was to promote national security.

This article interrogates the right to privacy and mass digital surveillance, and the legality and implications of mass digital surveillance in Uganda. Chapter one discusses the introduction, chapter two discusses the nature of surveillance, chapter three discusses the genesis of mass digital surveillance, chapter four discusses the right to privacy and mass digital surveillance, chapter five discusses the legality of mass digital surveillance, chapter six discusses the implications of mass digital

[1] Neil M. Richards, "The Dangers of Surveillance", (2013), 126, Harvard Law Review, p. 1934.
[2]Elizabeth Kamurungi, 'Car trackers: Govt assures on privacy', *Daily Monitor* (Kampala, 26 July 2021), at:
<www.monitor.co.ug/uganda/news/national/car-trackers-govt-assures-on-privacy--3487014>accessed 22 June 2022.
[3]Ibid.
[4]Ibid.
[5] Elias Biryabarema,'Ugandan opposition, activists denounce digital car tracker plan', *Reuters* (29 July 2021) < www.reuters.com/world/africa/ugandan-opposition -activists-denounce-digital-car-tracker-plan-2021-07-29/> accessed 22 June 2022.

surveillance, chapter seven discusses the recommendations and chapter eight discusses the conclusion.

2. NATURE OF SURVEILLANCE

2.1. Concept of Surveillance

The term surveillance has been used in different ways. A literal definition of surveillance as watching over indicates monitoring the behaviour of persons, objects, or systems. However, surveillance is not the only visual process that involves looking at people and things. Surveillance can be performed in a wide range of ways using a variety of technologies.[6]

Surveillance has been conducted by governments throughout history. Several surveillance methods have been developed over the years, from face to face, paper-based modes to increasingly sophisticated computer-based pervasive monitoring systems.[7] Surveillance instruments include closed-circuit television (CCTV), the interception of telecommunications commonly known as wiretapping in the United States of America, heat-seeking and other sensing devices, body scans, technology for tracking movement, and many others.[8]

2.2. Types of Surveillance

There are two broad types of surveillance to wit; mass and targeted.[9]

2.2.1. Mass Surveillance

Mass surveillance does not target any individual but gathers images and information on the entire population for possible future use. CCTV is an example of mass surveillance.[10]

2.2.2. Targeted Surveillance

Targeted surveillance is directed at specific individuals. Targeted surveillance can be performed overtly or covertly and can involve human agents.[11] Target surveillance can be carried out through the interception of communications, the use of communication traffic data, visual surveillance devices, and devices that sense the movement of objects or persons.[12]

---

[6] Constitution Committee, 'Surveillance and the State' <publications.parlaiment.uk/pa/Id200809/Idselect/Idconst/18/1804.htm > accessed 20 July 2022.
[7] Mark Anderson et al, 'Does Mass Surveillance by Governments matter?' <www.southampton.ac.uk/mwra1g13/msc/comp6048/governnment-mass-surveillance.html > accessed 12th July 2022.
[8] Supra (no.6).
[9] Supra (no.6).
[10] Supra (no.6).
[11] Supra (no.6).
[12] Supra (no.6).

3. GENESIS OF MASS DIGITAL SURVEILLANCE

3.1. Mass Digital Surveillance

Mass digital surveillance is indiscriminate surveillance that uses systems or technologies that collect, analyze, and generate data on indefinite or large numbers of people instead of limiting surveillance to individuals for whom there is reasonable suspicion of wrongdoing. [13] Mass digital surveillance can subject a population or significant component thereof to indiscriminate monitoring, involving systematic interference with people's right to privacy and all other attendant rights enabled by the right to privacy, including the freedom to express yourself and to protest. [14]

Mass digital surveillance is carried out by intelligence agencies and law enforcement in a number of ways, including direct mass interception of communications, access to bulk communications stored by telecommunication operators, mass hacking, indiscriminate use of facial recognition technology, and indiscriminate surveillance of protests using mobile phone trackers.[15]The proposed real-time tracking of the movement of motor vehicles, motor cycles, and boats by the government is a form of mass digital surveillance that will enable governments through intelligence agencies and law enforcement to capture virtually all aspects of our lives.[16]

3.2. Evolution of Mass Digital Surveillance

Mass digital surveillance has evolved in the recent past with the emergence of new and advanced technologies.[17]The emergence of these technologies, which has made it easy for governments and private actors to carry out mass digital surveillance. Previously, governments and private actors were unable to carry out mass digital surveillance and opted for targeted digital surveillance because of the high cost of mass digital surveillance because of the development of technology at the time.

Commentators exploring the emergence of technologies in the recent past provide contextualization of mass digital surveillance, suggesting a growing desire for governments to exert stricter social control over their citizens. [18]

[13]Privacy International, 'Mass Surveillance'<www.privacyinternational.org/learn/mass-surveillance> accessed 22 June 2022.
[14]Ibid.
[15]Ibid.
[16]Ibid.
[17] These include facial recognition software; closed circuit television (CCTV); social media platforms like Facebook; Twitter; Instagram and Snapchat and global positioning system (GPS).
[18] Mark Anderson et al, 'Does Mass Surveillance by Governments matter?' <www.southampton.ac.uk/mwra1g13/msc/comp6048/governnment-mass-surveillance.html > accessed 12th July 2022.

3.3. Contemporary Mass Digital Surveillance

Mass digital surveillance, as we know today, is a result of the September 11 terrorist attacks in the United States of America and stems from the need to safeguard against future terrorist attacks. The Government of the United States of America post the September 11 terrorist attacks through its enactment of the Patriotic Act 2001 embarked on several mass digital surveillance programs overseen by the National Security Agency mainly targeting citizens and foreign nationals with ties to countries in the Middle East and Muslim majority countries.[19]

This mass digital surveillance took the form of eavesdropping commonly known as wiretapping in the United States of America on all outgoing and incoming international phone calls from Middle East and Muslim majority countries to citizens and foreign nationals living in the United States of America.[20] This blueprint by the Government of the United States of America has been adopted wholly or with modifications by different governments worldwide that have gone on to embark on mass digital surveillance of their citizens claiming to do so for national security and public safety purposes.[21]

The Ugandan Government's proposed mass digital surveillance is not the first in the world; however, one could argue that it is the first in the East African region or at least it is the first to be publicly done by the government owing to allegations that the Rwandan Government, with the help of Pegasus mass digital surveillance software, has been secretly spying on key figures in the Ugandan Government and its critics within the country and abroad.[22]

4. THE RIGHT TO PRIVACY AND MASS DIGITAL SURVEILLANCE

4.1. Right to Privacy

4.1.1. Right to Privacy under the 1995 Constitution

The 1995 Constitution provides the right to privacy [23] in general. This right has been expounded by Courts and applied to various scopes of private life, including the sphere of technology. In *Ayena Odongo v The Pepper Publication,*[24] the Court

[19] ACLU v NSA, 493 F.3d 644 (6th Cir. 2007).
[20] Ibid.
[21] This is demonstrated by a number of decisions of the European Court of Human Rights regarding the legality of mass surveillance that include: *Centrum For Rattvisa v Sweden* App no 35252 of 2008 (ECtHR , 25 May 2021); *Szabo and Vissy v Hungary* App no 37138 of 2014 (ECtHR, 12 January 2016); *Liberty and Others v United Kingdom* App no 58243 of 2000 (ECtHR, 1 July 2008); *Weber and Saravia v Germany* App no 54934 of 2000 (ECtHR, 29 June 2006); *Roman Zakharov v Russia* App no 47143 of 2006 (ECtHR, 4 December 2015); *Telegraaf Media Nederland Landeliike Media B.V. and Others v The Netherlands* App no 39315 of 2006 (ECtHR, 22 November 2012); *Kennedy v United Kingdom* App no 26839 of 2005 (ECtHR, 18 May 2010) and *Big Brother Watch and Others v United Kingdom* App no's 58170 of 2013, 62322 of 2014 and 24960 of 2015 (ECtHR, 25 May 2021).
[22] Michela Wrong , 'Rwandans have long been used to Pegasus-style surveillance' The Guardian (London , 23 July 2021)<www.theguardian.com/commentisfree/2021/jul/23/rwanda-pegasus-surveillance >accessed 20 July 2022.
[23]Article 27.
[24] Miscellaneous Cause Number 08 of 2016.

observed that the photographing of the Applicant by the photographer of the Respondent in an enclosed private place without his consent and publishing the same amounted to a violation of the Applicant's right to privacy because he had a reasonable expectation of privacy.

4.1.2. Right to Privacy under the ICCPR

The ICCPR provides that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy"[25] and The Human Rights Committee in General Comment 16 on the Right to Privacy expounded the scope of the right to privacy and extended it to the technology sphere.[26] The Human Rights Committee states that the gathering and holding of personal information on computers, data banks, and other devices by public authorities must be regulated by law, and that effective measures have to be taken by states to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process, and use it, and is never used for purposes incompatible with the right to privacy.[27]

4.2. Convergence of the Right to Privacy and Mass Digital Surveillance

The right to privacy and mass digital surveillance converges under the auspices of the right to data privacy and protection. While data privacy and protection are not always directly mentioned as separate rights in constitutions, nearly all states recognize their value as a matter of constitutional significance. [28]Although the right to data privacy and protection is enshrined in the 1995 Constitution[29] and the International Covenant on Civil and Political Rights (herein after referred to as the ICCPR), [30]the applicability and enforceability of the right has, until recently, been a laughable notion in Uganda. [31]

The enactment of the Data Protection and Privacy Act 2019 and the Data Protection and Privacy Regulations 2021 has gone a long way in galvanizing and enforcing the right to data privacy and protection in Uganda. However, given that the Act and Regulations have recently been enacted, they have not yet been tested in the Ugandan Courts of Law. A challenge of the government's intended mass digital surveillance in the Ugandan Courts of Law will grant the courts an opportunity to render its pronouncement on the extent of the applicability of the above-mentioned data protection and privacy laws in Uganda. Something that is highly anticipated and welcomed.

At the continental level, the African Union (AU), recognizing the need to regulate data privacy and protection, introduced the Convention on Cyber Security and Personal Data Protection in 2014. As expected, only a handful of AU member states have assented to the convention or enacted local data protection regulations,

[25]International Covenant on Civil and Political Rights, Article 17.
[26]HRI/GEN/1/Rev.9 (Vol. 1), Paragraph 10.
[27]Ibid.
[28]Kenneth Muhangi, "Overview of the Data Protection Regime in Uganda" (2019) 3, Journal of Data Protection and Privacy, at p. 2.
[29]Article 27.
[30]Article 19.
[31]Supra, (no.14), p.2.

leaving Uganda as one of only a few elite African nations to regulate data protection and privacy.[32] Mass digital surveillance is synonymous and intertwined with personal data collection and processing, bringing it to the ambit of the right to data privacy and protection in specific terms and the right to privacy in general terms. Surveillance and data collection are features of almost every aspect of the public sector. The processing of personal data has always been part of public administration and is essential for effective governance and efficient service delivery. [33]

Contemporary uses of surveillance and data collection or processing can, however, be distinguished from those of the past in terms of extent and intensity, with which information is analysed, collated, and used.[34] Mass digital surveillance involves the use of personal data use, sharing, matching, mining, and profiling. Personal data use involves the processing and collection of personal data. [35]Personal data sharing involves the transfer of personal data from one entity or an individual to another.[36] Personal data matching involves comparing different sets of personal data to identify common features or trends in personal data.[37] Personal data mining involves the use of mathematically based analytical tools to detect patterns in large sets of personal data with the intent of predicting certain types of behaviour.[38] Personal data profiling involves the inference of a set of characteristics of a particular class of people based on their past experiences, as evidenced by their personal data.[39]

5. LEGALITY OF MASS DIGITAL SURVEILLANCE

5.1. Mass Digital Surveillance Violates Rights

5.1.1. Right to Privacy

Mass digital surveillance violates the right to privacy guaranteed by the 1995 Constitution [40]and the International Covenant on Civil and Political Rights[41] as it arbitrarily and unlawfully interferes with individuals' privacy. This is so much so because mass digital surveillance is not authorized by law [42] and covers an unlimited scope of the target's private life.[43] Sotomayor J in her concurring opinion

[32] Ibid.
[33] Constitution Committee, 'Surveillance and the State', at:
<publications.parlaiment.uk/pa/Id200809/Idselect/Idconst/18/1804.htm > accessed 20 July 2022.
[34] Ibid.
[35] Supra (no.33).
[36] Supra (no.33).
[37] Supra (no.33).
[38] Supra (no.33).
[39] Supra (no.33).
[40]Article 27.
[41]Article 17.
[42] In *United States of America v Jones* 565 U.S. 400(2012), the United States Supreme Court observed that a surveillance device had been placed on Mr. Jone's vehicle to monitor his movements without authorization by law.
[43]In *Szabo and Vissy v Hungary* App no 37138/2014 (ECtHR, 12 January 2016), the European Court of Human Rights observed that the mass surveillance program by the government of Hungary could include virtually anyone in Hungary and that with new technologies enabling the government to

in the *United States v Jones*,[44] observed the following about surveillance and the right to privacy:

> In this case, the Government installed a Global Positioning System (GPS) tracking device on respondent Antoine Jones' Jeep without a valid warrant and without Jones' consent, then used that device to monitor the Jeep's movements over the course of four weeks. The Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to Fourth Amendment Protection.[45]

What the Ugandan Government's proposed mass digital surveillance intends to do is in material respect, similar to what the United States Government did in the above case, albeit on a larger scale and for an infinite period. If the Government goes ahead with its plans and implements the same, it will violate the right to privacy of the Ugandans, as guaranteed by Article 27 of the 1995 Constitution.

5.1.2. Freedom of Movement

Mass digital surveillance has a chilling effect on the right to freedom of movement guaranteed by the 1995 Constitution[46], the African Charter on Human and Peoples Rights, [47] and the International Covenant on Civil and Political Rights[48], as it prohibits individuals from going about their daily routines and movements due to fear of being watched by authorities.

The right to freedom of movement presupposes liberty and freedom to move wherever and whenever one wishes. Mass digital surveillance takes away this as often individuals may fear making certain movements to various destinations for fear of being associated with those destinations or for fear that their movements will not go well with the authorities.

Members of the opposition parties, critics of government, and gender or sexual minorities will not be able to freely move about the country due to the proposed surveillance given the track record of security agencies towards them.

5.1.3. Freedom of Association

Mass digital surveillance curtails the right to freedom of association guaranteed by the 1995 Constitution,[49] the African Charter on Human and Peoples Rights, [50] and the International Covenant on Civil and Political Rights[51], as it prevents individuals from associating for fear of being in trouble or persecuted by the authorities.[52]

---

intercept masses of data easily concerning even persons outside the original range of operation.

[44]565 U.S. 400 (2012).

[45]565 U.S. 400 (2012) at p.1.

[46]Article 29.

[47]Article 12.

[48]Article 12.

[49]Article 29.

[50]Article 10.

[51]Article 22.

[52] This is especially so with minorities in society who are often times prohibited from associating

The cornerstone of the right to freedom of association is the ability and possibility to associate with whomever one wishes, whenever, and wherever one wishes. Mass digital surveillance takes away this, as often times individuals may fear associating with others who are subject to surveillance for fear of being associated with them and being presumed guilty.

Sotomayor J in *United States v. Jones*,[53] observed that awareness that the government may be watching chills associational freedoms. There are concerns that members of the opposition parties, critics of government, and sexual minorities will not be able to freely associate because of the proposed surveillance, which concerns are valid given the track record of security agencies towards them.[54]

5.1.4. Freedom of Assembly

Mass digital surveillance runs contrary to the right to freedom of assembly guaranteed by the 1995 Constitution,[55] the African Charter on Human and Peoples Rights, [56] and the International Covenant on Civil and Political Rights,[57] as it prevents individuals from freely assembling at their venue or location of choice because of fear of being persecuted by the authorities.[58]

The right to freedom of assembly necessitates liberty and freedom to assemble at one's preferred venue or location of choice. Mass digital surveillance takes this liberty and freedom as often as individuals fear assembling at a preferred venue or location of choice due to anticipation of surveillance from the authorities.

5.1.5. Freedom of Expression

Mass digital surveillance often triggers self-censorship by individuals in a bid to avoid surveillance, leading to a violation of the right to freedom of expression guaranteed by the 1995 Constitution[59] , the African Charter on Human and Peoples Rights, [60] and the International Covenant on Civil and Political Rights[61], which presupposes expression based on the free will of individuals, without any form of

with each other due to fear of being profiled and persecuted by the authorities as result of surveillance.

[53]565 U.S. 400 (2012) at p.3.

[54] Security agencies have notoriously dispersed gatherings of opposition parties invoking provisions of the Police Act and the Public Order Management Act 2013 which provisions and Act have been rendered unconstitutional by the Constitutional Court of Uganda in *Muwanga Kivumbi v Attorney General* [2008] UGCC 34 and Human Rights Network and 4 Others v Attorney General [2020] UGCC 6 ; Members of the LGBTQI community have equally had a number of their gatherings disrupted by security agencies especially in the aftermath of the enactment of the repealed Anti Homosexuality Act 2014. In *Nabagesera and 3 Others v Attorney Genera*l [2014] UGHCCD 85, a workshop of members of the LGBTQI community was dispersed by the Uganda Police for direct and indirect promotion of same sex practices contrary to the law and public interest.

[55] Article 29.

[56] Article 11.

[57]Article 21.

[58]In *Wood v Commissioner of Police for the Metropolis* [2009] EWCA Civ 414, the court observed that the secret photographing of the Appellant by the police as a result of his attending a meeting concerning arms trade on account of his opposition to arms trade had a chilling effect on not only his right to privacy but also his right to freedom of assembly.

[59]Article 29.

[60]Article 9.

[61]Article 19(2).

influence.

In particular, movement from one place to another is a form of expression, and the government's proposed mass digital surveillance will make a number of individuals restrict their movements for fear of being watched by authorities.

5.2. Mass Digital Surveillance is not Acceptable and Demonstrably Justifiable in a Free and Democratic Society

For mass digital surveillance to be acceptable and demonstrably justifiable in a free and democratic society, in light of the 1995 Constitution,[62] it must satisfy the tripartite test of being legal, necessary and proportionate.[63]

5.2.1. Legality of Mass Digital Surveillance

Mass digital surveillance meets the legal requirement if imposed by law. The law in question must be with sufficient precision and not vague, must have safeguards to prevent abuse, such as an assessment should be made at each stage of the process to ensure the necessity and proportionality of measures being taken, that mass surveillance is subject to independent authorization at the outset, the object and scope of the surveillance are being defined, and that the surveillance should be subject to supervision and independent ex post facto review. [64]

The relevant existing legal regime in Uganda, that is, the Regulation of Interception of Communications Act 2010 and the Data Protection and Privacy Act 2019, does not sanction mass digital surveillance but only individual or group surveillance, as discussed below, since it does not envision a situation necessitating the surveillance of Ugandans en mass even for national security and public safety considerations.

As such, mass digital surveillance that is not sanctioned by law does not meet the requirement of legality and is thus not demonstrably justifiable in a free and democratic society like Uganda.

5.2.2. Necessity of Mass Digital Surveillance

Mass digital surveillance meets the necessity requirement if it aims to achieve a legitimate objective. It is not sufficient for the government to claim good intentions in a bid to demonstrate the need to achieve a legitimate objective. The necessity visa against the legitimate objective must be evidence-based and rational.[65] In *Digital Rights Ireland Limited v Minister for Communications, Marine and Natural Resources,*[66] the Court of Justice of Europe (hereafter referred to as the CJEU) observed that an interference may be justified when it pursues an objective

[62]Article 43(2)(c).

[63]In *Charles Onyango Obbo v Attorney General* [2004] UGSC 1, the late Mulenga JSC observed that a Court in determining what is acceptable and demonstrably justifiable in a free and democratic society in light of Article 43 (2) (c) will have to make an analysis on whether the limitation of rights in question satisfies the tripartite test of being legal, necessary and proportional.

[64]*Big Brother Watch and Others v United Kingdom* App no's 58170 /2013, 62322/2014 and 24960 /2015 (ECtHR, 25 May 2021).

[65]Umuhoza v Rwanda [2018] AfCHPR 5.

[66] C-293/12 (ECJ, 8 April 2014).

of general interest, such as a fight against crime and, ultimately, public security.

In *Tele 2 Sverige AB v Post*,[67] the CJEU observed that legislation for purposes of fighting crime provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. According to the Court, such legislation exceeds the limits of what is strictly necessary and cannot be considered justified within a democratic society. In *Frantisek Rynes v Urad Pro Ochranu Osobnich Udaju*,[68] the CJEU noted that the protection of the fundamental right to private life requires that derogations and limitations in relation to the protection of personal data apply as far as is strictly necessary.

In *Prokuratuur*,[69] the CJEU noted that only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying that public authorities have access to a set of traffic or location data that are liable to allow precise conclusions to be drawn concerning the private lives of the persons concerned.

The government's claims that the proposed mass digital surveillance will curb crime and is thus necessary cannot be supported by empirical evidence, especially given the fact that the registration of all mobile phone users in the country in a bid to curb crime has not yielded any results on that front. For similar reasons as the registration of all mobile phone users, the proposed mass digital surveillance will not curb crime, because there is no guarantee that criminals will use motor vehicles, motorcycles, or boats registered in their names to commit crimes, just as they currently do not use mobile phones registered in their names.

In *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*,[70] the CJEU observed that obligations to forward data to security and intelligence agencies in a general and indiscriminate way constitute serious interference to the fundamental right to private life where there is no link between the conduct of the persons whose data are affected, and the objective pursued by the legislation at issue.

5.2.3. Proportionality of Mass Digital Surveillance

Mass digital surveillance meets the proportionality requirement if it is the least intrusive measure of the enjoyment of rights. This is known as the Oakes test, which was formulated by the Canadian Supreme Court in the case of *R v Oakes*[71] and adopted by numerous courts across different jurisdictions.[72] In *Digital Rights Ireland Limited v Minister for Communications Marine and Natural Resources*,[73] the CJEU rendered a directive of the European Union (hereinafter referred to as the EU) invalid on the grounds that the wide-ranging and particularly serious interference with the fundamental rights to respect for private life and protection of personal data that it entailed was not sufficiently circumscribed to ensure that that

[67] C-203/15 (ECJ, 21 December 2016).
[68] C-212/13(ECJ, 11 December 2014).
[69] C-746/18(ECJ, 2 March 2021).
[70] C-623/17(ECJ, 6 October 2020).
[71][1986] 1 SCR 103.
[72]This decision was adopted by the Ugandan Supreme Court in Charles Onyango Obbo and Another v Attorney General [2004] UGSC 1.
[73] Supra (no.66).

interference was limited to what was strictly necessary. The directive covered, in a generalized manner, all persons and all means of electronic communication, as well as all traffic data without any differentiation, limitation, or exception being made in light of the objective of fighting serious crime. The directive also failed to lay down any objective criterion by which to ensure that competent national authorities would have access to the data and be able to use them for the sole purpose of preventing, investigating, and prosecuting offences capable of being considered sufficiently serious to justify interference.

In *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*,[74] the CJEU retaliated that national legislation is precluded from requiring providers of electronic communications services to carry out the general and indiscriminate transmission of traffic and location data to security and intelligence agencies to safeguard national security.

In *Big Brother Watch v United Kingdom*,[75] the European Court of Human Rights laid down elements of proportionality that should be considered when carrying out surveillance to include:

- Balancing the size and scope of the proposed interference against what was sought.
- Explaining how and why the adopted methods will cause the least possible intrusion on the subject and others.
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, consider all reasonable alternatives to obtain the necessary result.
- Evidencing, as far as reasonably practicable, other methods have been considered and were either not implemented or have been employed, but which were assessed as insufficient to fulfil operational objectives without the addition of the intercept material sought.

Thus, it is suggested that the proposed mass digital surveillance is not proportionate on the following grounds:

- It is broad and encompassing, that is to say, it covers everyone and goes against the universal standard of covering only those reasonably believed to have committed or about to commit a crime. [76]
- It is not authorized through a court-issued warrant as required by the Regulation of Interception of Communications Act 2010.[77]
- It does not provide for the scope and time frame of surveillance as it will be in real time 24 h, 7 days a week, covering all movements of the population.
- There are no exceptions, such as surveillance not being carried out when individuals are going to places of worship, dropping off their children to school, travelling to their homes, or going to a hospital for treatment. [78]

The proposed mass digital surveillance system does not have safeguards for the abuse of power by the government. The European Court of Human Rights has

[74] Supra (no.70).
[75]App no's 58170 /2013, 62322/2014 and 24960 /2015 (ECtHR, 25 May 2021).
[76]*United States of America v Jones*, 565 U.S. 400 (2012).
[77]Section 2.
[78]In *United States of America v Jones*, 565 U.S. 400 (2012), the Federal District Court excluded surveillance data covering Mr. Jone's home from forming part of the trial evidence.

proposed several safeguards in place to prevent abuse of power, including:

- The nature of offences which may give rise to an interception order.
- The definition of the categories of the categories of people liable to be surveilled.
- A limit on the duration of surveillance.
- The procedure to be followed for examining the surveillance data.
- The precautions to be taken when communicating the surveillance data to other parties.
- The circumstances in which surveillance data may or must be erased or destroyed.[79]

None of the above safeguards are provided by the proposed government mass surveillance, leading to the conclusion that the same is not proportional.

5.3. Mass Digital Surveillance does not Meet the Requirements of the Data Protection and Privacy Act 2019

The Data Protection and Privacy Act, 2019 (hereafter referred to as the Act) authorizes collection of personal data without the consent of the data subject, "where it is necessary for the proper performance of a public duty by a public body, for national security and for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law."[80]

The Government creates a case in which the proposed mass digital surveillance is for national security purposes. This raises the question of what forms of surveillance fall within the national security exception. The concept of national security can be zeroed down to a country's ability to protect itself from violence or attack. [81] Surveillance can be one way in which a country can protect itself from violence or attacks.

In *European Parliament v Council of the European Union*,[82]the CJEU observed that passenger name records collected and provided by airlines operating flights to and from and within the United States to the Government furthered national security purposes. So, what form of surveillance can achieve the above-mentioned goal is the question? It is submitted that legally sanctioned and targeted surveillance,[83] and not mass digital surveillance, given that the entire act read as a whole does not permit mass digital surveillance.

In *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*[84], the CJEU observed that legislative measures that allow recourse to targeted retention, limited in time to what is strictly necessary, of traffic and location data, are not precluded by the fundamental right to private life. The CJEU

[79] *Big Brother Watch and Others v United Kingdom* App no's 58170 /2013, 62322/2014 and 24960 /2015 (ECtHR, 25 May 2021).

[80] Data Protection and Privacy Act 2019, s.7(2)(b).
[81] www.collinsdictionary.com/dictionary/englsih/nationalsecurity accessed 11 September 2022.
[82] C-540/03 (ECJ, 27 June 2006).
[83] Surveillance targeting a particular individual or group of people suspected of having committed a crime or of about to commit a crime.
[84] Supra (no.74).

further observed that legislation that requires providers of electronic communications services to have recourse to real-time collection of traffic and location data, where that collection is limited to persons with whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to prior review carried out either by a court or by an independent administrative body whose decision is binding, to ensure that such real-time collection is authorized only within the limits of what is strictly necessary, is not precluded by the fundamental rights to private life.

The targeted surveillance chosen by the government could take the form of physical surveillance by security operatives or digital surveillance using global positioning system tracking devices placed on vehicles, mobile phones through chips, tapping into phone calls, email conversations, and any other way. It is mortifying, one may say, that the Section 7 of the Data Protection and Privacy Act 2019 should not be read in isolation from other sections in the same Act, as it is a cardinal rule of statutory interpretation that the entire statute should be read as a whole.[85]

The same Act prohibits obtaining data in a manner that violates the right to privacy, regardless of any national security considerations.[86]Mass; mass digital surveillance is clearly a violation of the right to privacy, as discussed earlier, and thus is not permitted by the Act even for national security considerations.

The Act equally elaborates on the data protection principles, [87] which include accountability to the data subject for data collection, fair and lawful collection and processing of data collection and processing of relevant and not excessive or unnecessary personal data, retaining personal data for the period authorized by law or for which the data is required, and ensuring transparency and participation of data subjects in the collection, processing, use, and holding of personal data.

In *Big Brother Watch v United Kingdom*,[88] the European Court of Human Rights observed that each of the intelligence services was a "data controller" for the purposes of the DPA and, as such, they were required to comply with the data protection principles.

The Government of Uganda is thus enjoined to observe the data protection principles stipulated in the Data Protection and Privacy Act 2019, and the government's proposed mass digital surveillance runs contrary to all the above stated data protection principles; thus, its implementation will be unlawful for being contrary to the Data Protection and Privacy Act 2019. It is quite ironic that the same government mandated to ensure that the data protection principles comply with is the same and does not intend to comply with them.[89]

Furthermore, the Act provides that only data relevant to the legitimate aim of promoting national security can be obtained and processed by incorporating the data minimality and proportionality principle into the Act. Given that mass digital surveillance enables the acquisition and processing of data that are not relevant to

[85]*Uganda Revenue Authority v Kajura* [2017] UGSC 63.
[86]Data Protection and Privacy Act 2019, s.10.
[87]Data Protection and Privacy Act 2019, s.3.
[88]App numbers 58170 /201, 62322/2014 and 24960 /2015 (ECtHR, 25 May 2021).
[89]Section 3(2) of the Data Protection and Privacy Act 2019 gives the National Information Technology Authority a government agency the mandate (which mandate is mandatory given the use of the word "shall") to ensure that every data collector, data controller, data processor or any other person collecting or processing data complies with the principles of data protection in the Act.

the legitimate aim of promoting national security due to its real time and unlimited length, it cannot be permitted by the Act, even for national security purposes.

Finally, the Act equally prohibits unlawful obtaining and disclosure of personal data.[90] This means that data can only be obtained even for national security purposes in a manner that is prescribed by the law, which in this case would be the elaborate procedure prescribed by the Regulation of the Interception of Communications Act.[91]

5.4. Mass Digital Surveillance does not comply with Regulation 12 Data Protection and Privacy Regulations 2021

Uganda's Data Protection and Privacy Regulations 2021 provide for a data protection impact assessment prior to the collection or processing of personal data in situations where the collection or processing of personal data poses a high risk to the rights and freedoms of natural persons.[92] The use of the word "shall" in regulation 12 connotes that the data protection impact assessment is mandatory and must be carried out prior to the collection or processing of personal data.

From the discussion above, the collection and processing of personal data under the proposed mass digital surveillance pose a high risk to the rights and freedoms of natural persons, necessitating the need for a data protection impact assessment prior to the implementation of the same. It is not clear at the moment whether the government has conducted a data protection impact assessment, and in the absence of that clarity, if the proposed mass digital surveillance is carried out, it would be in violation of the regulations.

5.5. Mass Digital Surveillance is not Authorized by the Regulation of Interception of Communication Act 2010

The Regulation of Interception of Communications Act 2010 states that no person intercepts any communication unless he or she is authorized by a warrant.[93] A party seeking to intercept any communication needs to apply to a designated Judge [94]and the Judge can only grant after being satisfied after an examination of the evidence that the subject of a warrant has committed crime or is likely to commit a crime.[95]

[90] Data Protection and Privacy Act, s.35.
[91]Regulation of Interception of Communications Act, s.4 and s.5.
[92] Data Protection and Privacy Regulations 2021, r.12.
[93] Regulation of Interception of Communications Act, s.2.
[94] Regulation of Interception of Communications Act, s.4. A designated judge is defined in Section 1 as a Judge designated by the Chief Justice to perform the functions of designated judge for the purposes of the Act. No judge has been designated by the Chief Justice in accordance with that section which means that no application for a warrant can be made or granted in accordance with the Act making any digital surveillance illegal even when it is justifiable in accordance with the Act.
[95]Regulation of Interception of Communications Act, s.5.

6. FURTHER IMPLICATIONS OF MASS DIGITAL SURVEILLANCE

6.1. Enables Profiling

Mass digital surveillance enables state authorities to sort the public into categories of people,[96]depending on a given criterion, and in this particular case, it will be based on their movements. The intended government mass digital surveillance will enable state authorities to mark the general public's movement patterns and regular visits, which will be a tool for profiling the members of the public.

This can be a disadvantage for many people, especially those belonging to minority groups.[97]

6.2. Fosters the Presumption of Guilt

Mass digital surveillance fosters the presumption of guilt, as it enables state authorities to intentionally target a particular individual or group of people who they believe or presume to be engaged in unlawful activities without legal justification.[98]

6.3. Precipitates Blackmail and Extortion

Mass digital surveillance enables the acquisition of vast information about the members of the public, which, if in the wrong hands, can lead to blackmail and extortion of members of the public, especially if it is embarrassing, portrays immorality, or individuals' secrets. [99]

Sotomayor J in the *United States v. Jones* [100] described the nature of information that can be acquired in the following terms:

> Disclosed in GPS data will be trips the indisputably private nature of which takes little imagination to conjure trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment centre, the strip club, the criminal defence attorney, the by-the hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.[101]

One can only imagine the effect of information regarding a married public figure's rendezvous at a hotel, lodge, or inn with someone other than their spouse being exposed,[102] information regarding one being a member of the LGBTQI

[96]Neil M. Richards, "The Dangers of Surveillance", (2013), 126, Harvard Law Review, p. 1956.
[97] In Uganda and many other parts of the world, we have seen incidences where mosques are raided, and Muslims arrested after terrorist attacks due to profiling.
[98] In *United States v Jones* 565 U.S. 400 (2012), Mr. Jones was subjected to unauthorized electronic surveillance on grounds of his previous criminal conduct.
[99]Supra, The Dangers of Surveillance, p.1953.
[100] 565 U.S. 400 (2012).
[101] *United States v Jones* 565 U.S. 400 (2012) at p.3.
[102] In *Ayena Odong v The Pepper Publications* Miscellaneous Cause Number 08 of 2016, the Applicant a Member of Parliament sued the Respondent for publishing photos and stories about him

community being made public,[103] and information regarding a public figure visiting a shrine making headlines.[104]

7. COMPARATIVE ANALYSIS WITH OTHER JURISDICTIONS

7.1. Southern Africa

In the Southern Region of Africa, South Africa was very notorious for surveillance during the apartheid regime that Africans were heavily surveilled by the secret police due to fear that they were members of the African National Congress and active participants in its armed struggle under its military wing known as "Umkhonto we Sizwe or Spear of the Nation."

The coming to power of the African National Congress to some extent, the scaling down of state surveillance in South Africa due to the peace that ensued. This can partly be attributed to the fact that South Africa, as a member state of the Southern Africa Development Community (hereafter referred to as SADC), is duty bound to implement the SADC Model Law.

Data Protection, which offers guidance on data protection legislation that member states should enact.

7.2. Europe

Edward Snowden's revelations against the National Security Agency equally incriminated some of its partners, chief among them being the United Kingdom Government Communications Headquarters (hereafter referred to as the GCHQ).

In *Big Brother Watch and Others v United Kingdom*, the Court observed that Edward Snowden revelations made in 2013 indicated that GCHQ was running an operation codenamed "Tempora," which allowed it to tap into and store huge volumes of data from Internet communications.

The Court equally observed that the GCHQ requested intelligence from the National Security Agency under the Interception of Communications Code of Practice under the "PRISM" and "UPSTREAM" operations.

The Court held that the actions of the GCHQ violated the right to privacy of the individuals that were the subject of these interceptions. Other European countries have equally carried out surveillance on their citizens, which has been rendered to be a violation of their citizens' right to privacy by the European Court of Human Rights.[105]

---

having an extra marital affair.

[103] In *Kasha Jacqueline and Others v Rolling Stone and Another* Miscellaneous Cause Number 163 of 2010, the Applicants who were members of the LGBTQI community sued the Respondents for publishing them in their magazine as members of the LGBTQI community without their consent exposing them to homophobia and threats to life.

[104]Even though Uganda is a secular state pursuant to Article 7 of the 1995 Constitution, the general population in the country is predominantly Christian and disdains public figures that embrace African Traditional Religion. The former Speaker of Parliament the Rt Hon Rebecca Alitwala Kadaga made headlines when she visited a shrine in her constituency and her claims that she was celebrating her heritage fell on deaf ears.

[105] *Centrum For Rattvisa v Sweden* App no 35252 of 2008 (ECtHR , 25 May 2021) ; *Szabo and*

7.3. Asia

In Asia, China is notoriously known for its ambition to collect staggering amounts of personal data from everyday citizens. An investigation by the New York Times reveals that phone tracking devices are now everywhere with the authorities building upon facial recognition technology to collect voice prints from the public. [106]

7.4. United States of America

The 2013 revelations by Edward Snowden of the scope and magnitude of electronic surveillance programs run by the United States National Security Agency (herein after referred to as the NSA) came at a time when the United States had long been believed to carry out surveillance of foreign nationals and its nationals in the aftermath of the September 11, 2001, terrorist attacks on the world trade centre in New York. [107]

Following the enactment of the Patriotic Act, the NSA carried out massive surveillance on the citizens of the United States and foreign nationals within and outside the United States in the guise of national security.

Before the Edward Snowden revelations, many individuals and organizations that went to court to challenge the actions of the NSA were unable to prove the existence of surveillance programmes and their cases were dismissed due to a lack of standing due to the failure to prove the existence of surveillance programmes and thus a legal grievance. The case in point is that of the American Civil Liberties Union v National Security Agency,[108] which was dismissed by the Sixth Circuit of the United States Court of Appeal.

In the United States [109], the Ninth Circuit of the United States Court of Appeal observed that the NSA's interception of Moalin's communications with Somalia was unconstitutional and contrary to the Foreign Intelligence Surveillance Act.

8. RECOMMENDATIONS

It is suggested that the best way for the government to achieve its intended objective is to carry out discrete individual and group surveillance of those who have committed crimes or are reasonably suspected of or about to commit crimes

Vissy v Hungary App no 37138 of 2014 (ECtHR, 12 January 2016); *Liberty and Others v United Kingdom* App no 58243 of 2000 (ECtHR, 1 July 2008); *Weber and Saravia v Germany* App no 54934 of 2000 (ECtHR, 29 June 2006); *Roman Zakharov v Russia* App no 47143 of 2006 (ECtHR, 4 December 2015) ; *Telegraaf Media Nederland Landeliike Media B.V. and Others v The Netherlands* App no 39315 of 2006 (ECtHR, 22 November 2012); *Kennedy v United Kingdom* App no 26839 of 2005 (ECtHR, 18 May 2010) and *Big Brother Watch and Others v United Kingdom* App nos 58170 of 2013, 62322 of 2014 and 24960 of 2015 (ECtHR, 25 May 2021).

[106] Isabelle Qian, Muyi Xiao, Paul Mozur and Alexander Cardia, 'Four Takeways From a Times Investigation Into China's Expanding Surveillance State' The New York Times (New York, 21 June 2022) < www.nytimes.com/2022/06/21/world/asia/china-surveillance -investigation.html> accessed 11 September 2022.

[107] Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' [2015], Volume 56, Harvard International Law Journal, p.81.

[108] 493 F.3d 644 (6th Cir. 2007).

[109]No. 13-50572 (9th Cir. 2020).

within the confines of the law. This does not help the government's cause when everyone knows that they are being surveyed. Any reasonable person who engages in criminal activity will not do so, knowing that the government is tracking every movement. Those that are wise, however, will engage in criminal activity without the government's ability to track their movements by devising alternative means of transport that are not being tracked.

It cannot be stated with certainty that people who engage in criminal activity in Uganda are reasonable or wise, since I am not privy to the world of criminal activity. What I am certain, however, is that the government will best achieve its intended objective of ensuring public safety and national security through discrete individual and group surveillance done within the confines of the law and not through public mass digital surveillance.

Lastly, the Chief Justice ought to designate a judge for the purposes of Section 4 of the Regulation of Interception of Communications Act 2010 to operationalize the Act and enable legal interception of communications that fosters public safety and national security.

CONCLUSION

Mass digital surveillance can never be resorted to even during dire times. This is so much so, given its corrosive nature on the right to privacy due to the inability to draw a fine distinction between what part of the individuals' private life that it is subjected to is relevant and what part is not for national security purposes in the absence of a probable cause that the individuals are about to or have committed crimes.

The late Justice Ruth Bader Ginsburg, in her seminal letter of Monday, November 30, 1953, to the Editor of the Cornell Daily Sun titled Wiretapping: Cure Worse than Disease? In response to the United States Attorney General Herbert Brownell's proposal, Congress enacted a law allowing federal prosecutors to introduce wiretap evidence when trying espionage cases in response to recent "disclosures of successful communist espionage penetration in government"[110]put it more aptly in the following words:

> Of course, society is interested in apprehending criminals, but the protection of the innocent has always been basic to our concept of justice. Both these ends must be weighed and balanced as to their relative merits before any conclusion can be reached about Mr. Brownell's proposal to admit evidence obtained by wiretapping in federal criminal trials.
>
> What did the law students mean by telling us that we are faced with a rising "crime" wave? Were they speaking about an increase in the activities of gangsters and racketeers, or the growing number of cases in which individuals are being prosecuted for political crimes.
>
> Wiretapping may save the government investigators a good deal of time and effort by making it unnecessary to seek other sources of proof. A thorough investigation of cases may seem like a burdensome task, especially when the

[110]Ruth Bader Ginsburg, My Own Words (1st edn, Simon & Schuster, 2016) at p. 45.

> shortcut of wiretapping can achieve more immediate results.
>
> But, even if the situation today demands increased vigilance on the part of government, restraints on individual rights in the field of individual privacy can be a cure worse than the disease. We may be anxious to reduce crime, but we should remember that in our system of justice, the presumption of innocence is prime, and the law cannot apply one rule to Joe who is a good man, and another to John, who is a hardened criminal.
>
> The general good Mr. Brownell's proposal is expected to accomplish seems to me to be outweighed by the general harm it may well do.[111]

Wiretapping in the United States of America is the colloquial name given to digital surveillance, and the late Justice Ruth Bader Ginsburg's words, even though written more than 50 years ago, are in consonance with today's lived realities and aspirations not only in Uganda but the world over.

If the Government decides to carry out mass digital surveillance of Ugandans in the form of digital tracking of motor vehicles, motorcycles, and boats, it will not only act illegally but will subject Ugandans to the far-reaching consequences of mass surveillance. I do not know about you, but I am personally uncomfortable with that and presume that every right-thinking member of a free and democratic society that we are and cherish is equally not. As the late Justice Ruth Bader Ginsburg suggested, mass digital surveillance is indeed a cure worse than the disease.

[111]Ibid at pp. 46- 47.

PLANT BREEDERS' RIGHT TO FOOD AND NUTRITIONAL SECURITY IN AFRICA: PROSPECTS AND CHALLENGES

Sanatu Mustapha Alidu,[*] Samuel Oppong Abebrese[†] and Amina Moro[‡]

ABSTRACT

Plant breeding is the art, science and business of improving plants for the benefit of mankind. Plant breeding over the years has evolved from an art to a precise and sophisticated scientific technology. Breeding new varieties is a resource-intensive activity in terms of costs, infrastructure, genetic resources, and the breeders' knowledge and experience. However, plant varieties can be reproduced easily and quickly, which hinders breeders' need to secure return on investment. Plant variety protection (PVP) system gives the breeder the exclusive rights to exploits his/her new varieties and prevent others from doing so illegally for a period of time. A PVP system is an important tool to encourage the development and release of new varieties of plants, ensuring and promoting access to innovation, technology transfer, food security and genetic diversity. In meeting the Trade Related Aspects of Intellectual Property Rights (TRIPS) obligation of all World Trade Organization (WTO) members to provide either patent or an effective sui generis protection for plant varieties, many African countries have drafted a PVP legislations which few have begun implementation.

By establishing such PVP systems, African countries hope to incentivize breeding and the introduction of new varieties, allowing farmers to access a wide range of improved varieties to contribute to both economic development and food security. Yet, these developments are being strongly opposed by several civil society organizations (CSOs), which are of the opinion that, the proposed legal frameworks are unsuitable for most African countries. A key concern is that a PVP system merely favours the interests of commercial breeders and marginalizes smallholder farmers by impeding the traditional farming practices of using, exchanging and selling farm-saved seed. This misunderstanding between proponents and opponents of the ongoing regional harmonization processes have taken centre stage and can be found both at the regional and national levels in Africa. Many smallholder farmers in Africa have difficulties in accessing quality seed of genetically superior varieties through the formal seed system due to physical and financial constraints. These farmers may only access new varieties through the use and exchange of farm-saved seed. The challenge for African countries is to strike a balance between protecting the interests of breeders and maintain the incentive function of plant breeders' rights in the commercial market, while providing sufficient leeway to smallholder farmers that depend on informal sources for their seed security and survival.

[*] Department of Crop Science, Faculty of Agriculture, Food and Consumer Sciences, University for Development Studies, P. O. Box TL 1882 Tamale, Ghana. Email: msanatu@uds.edu.gh
[†] CSIR-Savanna Agricultural Research Institute, P.O. Box TL 52, Tamale, Ghana. Email: sam555oppa@yahoo.com
[‡] Department of Crop Science, Faculty of Agriculture, Food and Consumer Sciences, University for Development Studies, P. O. Box TL 1882 Tamale, Ghana. Email: moroamina51@gmail.com

1INTRODUCTION

Agriculture is by far the single most important economic activity in Africa. It provides employment for about two-thirds of the continents working population and contributes an average of 30 to 60 percent of each country's gross domestic product (GDP) [1]. It similarly accounts for about 30 percent of the individual country's export value [2]. Despite the fact that it is the home of 60% of the world's arable land, Africa is among the regions of the world with severe food and nutritional security issues. It is also the continent with the lowest yields of staple food crops [3]. Agriculture will continue to play a critical role in African countries' economy and require favourable policies to grow the sector to serve the continent and the world at large [4]. Improved seeds are fundamental input in agriculture, therefore, the right policies surrounding its access and use will go a long way to benefit Africa's agriculture.

Plant varieties were developed over centuries through the exchange of seeds and the sharing of knowledge among farmers. Even today this is the model of innovation and diffusion in agriculture that prevails in most developing countries. It is based on principles of common ownership, within a given community, and free access to materials and knowledge [5][6]. However, with the development of commercial plant varieties by seed companies, a new model of production and diffusion, based on Intellectual property rights, has emerged[7]. Plant varieties can be improved for numerous agronomic reasons, such as better yields, quality, and resistance to biotic and abiotic stresses. In modern agriculture, crop varieties are derived through plant breeding by mating two or more parental lines that contain desirable characteristics, and the target characteristics are measured over multiple generations under different environmental conditions. Among the progeny, individuals with desirable characteristics are selected, whereas individuals with undesired characteristics are eliminated from the breeding process. This process, repeated over many generations, can create favourable combinations of genetic variations in the next generation, resulting in superior varieties [8].

[1] Megan Sheahan and Christopher B Barrett, *Agriculture in Africa: Telling Myths from Facts. Directions in Development* (Washington, DC: World Bank doi:101596/978-1-4648-1134-0 2018); Xinshen Diao, Peter Hazell and James Thurlow, 'The Role of Agriculture in African Development' (2010) 38 World Development 1375 <http://dx.doi.org/10.1016/j.worlddev.2009.06.011>.

[2] Diao, Hazell and Thurlow (n 1).

[3] Vikash Raj Satyal, 'Agriculture in Africa-Transformation and Outlook' (2010) 11 Economic Journal of Development 144; Diao, Hazell and Thurlow (n 1).

[4] Diao, Hazell and Thurlow (n 1).

[5] Chidi Oguamanam, 'Breeding Apples for Oranges: Africa's Misplaced Priority Over Plant Breeders' Rights' (2015) 18 Journal of World Intellectual Property 165.

[6] Niels P Louwaars, 'Integrated Seed Sector Development in Africa : A Conceptual Framework for Creating Coherence Between Practices , Programs , and Policies' (2013) 26 Journal of Crop Improvement 39.

[7] Niels Louwaars and others, *Breeding Business* (Centre for Genetic resources Netherlands (CGN), Wageningen, Wageningen University and Research Centre 2009); Mercedes Campi, 'The Co-Evolution of Science and Law in Plant Breeding: Incentives to Innovate and Access to Biological Resources' (2018) 23 Journal of Intellectual Property Rights 198.

[8] Gary N Atlin, Jill E Cairns and Biswanath Das, 'Rapid Breeding and Varietal Replacement Are Critical to Adaptation of Cropping Systems in the Developing World to Climate Change' (2017) 12

However, plant varieties can be reproduced easily and quickly, and breeders need to secure their return to investment [9]. Plant breeders have various options to protect their ownership of new varieties, prevent outlawed practices and recover breeding costs from royalties. Such options motivate breeders and support further breeding activities that constantly provide farmers with the best varieties that satisfy consumer demand [10]. Plant variety protection is designed for plant varieties, and grants breeders' exclusive rights on propagating material (such as seeds) of new plant varieties that they have developed. A question that is normally asked is, does this offer the plant breeder the right to be in full control of his or her new variety? The answer always gives rise to a long and controversial arguments.[11]

These discussions have driven over the years by mainly the same concerns and, especially, some issues shaped the debate. First, granting IPR to plant breeders' aims at stimulating private investments, thus improving farmers' possibilities to use new plant varieties that are developed based on scientific breeding methods. Secondly, on the other hand, there are concerns with regard to the sustainable use of agriculture biodiversity, the rights of farmers, and also to food and nutrition security and human rights. Thirdly private investment tends to be focused on few crops of major economic importance, and on breeding strategies that do not particularly address of small-scale farmers in developing countries. Lastly, identified as the 'breeder' has the right to control the use of the plant variety. This concerns the rights of farmer to save, use, exchange and sell seed obtained from their own harvest, as far as protected varieties are concerned [12]. In other to qualify for the exclusive right, a variety must be new, distinct, uniform and a stable

2. OVERVIEW OF PLANT VARIETY PROTECTION

2.1. World

Globally, plant varieties are protected either by patents or an effective sui generis system. Few countries protect plant varieties with patents [13]. Many countries, including developing countries and countries in transition to a market economy, are considering the introduction of a system for the protection of new varieties of plants (PVP system). Most countries which have already introduced a PVP system have chosen to base their system on the International Convention for

Global Food Security 31 <http://dx.doi.org/10.1016/j.gfs.2017.01.008>; Itefa Degefa Alemu, 'Plant Breeding Methods : In Brief for Students' (2019) 3 International Journal of Zambrut 156; SVS Shastry, 'Rice Breeding in Retrospect' (2006) 91; Flavio Breseghello and Alexandre Siqueira Guedes Coelho, 'Traditional and Modern Plant Breeding Methods with Examples in Rice (Oryza Sativa L.)' (2013) 61 Journal of Agricultural and Food Chemistry 8277.

[9] Louwaars and others (n 7).

[10] Philippe Cullet, 'Pant Variety Protection in Africa: Towards Compliance with the TRIPS Agreement' (2001) 1 Journal ofAfrican Law 97.

[11] ibid.

[12] Caroline B Ncube, 'Intellectual Property and the African Continental Free Trade Area: Lessons and Recommendations for the IP Protocol' (2022) 21 Journal of International Trade Law and Policy 105.

[13] Campi (n 7).

the Protection of New Varieties of Plants (UPOV) convention in order to provide an effective and internationally recognized system[14]. UPOV is an intergovernmental organization with the objective of protecting new plant varieties by intellectual property rights (IPRs); the common form being plant breeders' right [15]. The first International Intellectual Property Convention was the 1883 Paris Convention for the Protection of Industrial Property. In this convention, agriculture was recognised as an area of enterprise in respect of which property rights could be secured, thus Article 1 (3) of the Convention had declared that:

> Industrial Property shall be understood in the broadest sense and shall apply not only to industry and commerce proper, but likewise to agricultural and extractive industries and to all manufactured or natural products, for example, wines, grain, tobacco leaf, fruit, cattle, minerals, mineral waters, beer, flower and flour. (Paris Convention for the Protection of Industrial Property, 1967)

The UPOV Convention encourage breeding in all plant genera and species and does not attempt to pre-determine for which genera and species breeding would be beneficial. This has given an opportunity and the promotional rise of new species or genera of plants in the world. In 1975, protection had been granted to varieties of approximately 500 plant genera or species, growing to around 900 by 1985 and over 1,300 by 1995 [16]. It is estimated that protection had been sought for varieties of more than 2,500 genera or species by 2008. The UPOV members are divided into older members (those who join before 1992) and newer members (those who became members at the later date), the year 1992 was where fairly stable membership were cut off and the start of a continuous expansion in membership. The older members were made up of 10 members namely: Australia, Canada, Hungary, Israel, Japan, New Zealand, Poland, South Africa, Switzerland and the United States of America. These were UPOV members as of 1992 [17]. Members who joined from 1993 to 2000 include Bulgaria, Czech Republic, Estonia, Kyrgyzstan, Republic of Moldova, Russian Federation, Slovakia, Slovenia and Ukraine and some Latin American countries (Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Paraguay and Uruguay) as well as Austria, China, Finland, Kenya, Norway, Portugal and Trinidad and Tobago, and Kenya [18]. As at the year 2021 UPOV had 78 members, 19 States and 1 intergovernmental organization have initiated the procedure for acceding to the UPOV Convention and 22 States and 1 intergovernmental organization which have been in contact with the Office of the Union for assistance in the development of laws based on the UPOV Convention.

The UPOV convention has been revised three times (1972, 1978 and 1991) since it came to effect in order to remain consistent with developments in the professional breeding sectors of member countries with new members eligible only

[14] Oguamanam (n 5); Bram De Jonge, 'Plant Variety Protection in Sub-Saharan Africa: Balancing Commercial and Smallholder Farmers' Interests' (2014) 7 Journal of Politics and Law 100.
[15] Graham Dutfield, 'The Role of the International Union for the Protection of New Varieties of Plants (UPOV)'.
[16] ibid.
[17] ibid.
[18] ibid.

to join the UPOV 1991 Act [19]. Positive impact has been reported in some member countries which includes an increase in breeding activities and the structure of the breeding industry, improved varieties, increase number of new varieties, development of international market and enhance access to foreign germplasm. It is noted that, since there is also significant cost involved in obtaining protection, breeders will not seek variety protection for their new varieties unless protection is necessary, and their varieties have true market value [20].

2.1.1. Importance of Plant Variety Protection

The general benefits of adopting a plant variety protection system are as follows:

- **Increase breeding activity and structure of the breeding industry**: The major aim of the UPOV system was to enhance and promote an increased in breeding activity and encouragement of new types of breeders, including private breeders, researchers and farmer breeders. This has promoted an increase in breeding activities in all countries and states that have accepted UPOV.
- **Improved varieties:** As the number of breeders increase, it enhances the improvement of the local varieties to solve problems in the society. Acceptance of UPOV will promote development of new, protect varieties that will satisfy farmers, growers, industry and consumers.
- **Increased number of new varieties:** The Impact Study provided information on how the number of new varieties increased after the introduction of plant variety protection. It was also demonstrated that membership of UPOV was associated with an increase in the number of varieties introduced by foreign breeders, particularly in the ornamental sector.
- **Development of international markets:** One of the benefits of plant variety protection is to encourage the development of new, improved plant varieties that lead to improved competitiveness in foreign markets.
- **Enhanced access to foreign germplasm:** In addition to providing improved competitiveness for farmers, growers and industry, access to foreign plant varieties is an important form of technology transfer that can also lead to enhanced domestic breeding programs as a result of the breeders' exemption.

2.2. Conditions for Granting PVP under the UPOV System

The UPOV's prescription of technical criteria for protection of plant varieties are: (1) newness, (2) distinctiveness, (3) uniformity and (4) stability [21]. A variety is considered to be new if at the date of filing the relevant application for registration as a variety, or where applicable on the priority date, the propagating or harvested material of the variety has not been sold or otherwise disposed of to any person by or with the consent of the breeder for the purpose of exploitation of the variety in the country in which protection is sought, earlier than one year before the date of

[19] Jonge (n 14); Campi (n 7); Dutfield (n 15); Chidi Oguamanam, 'Farmers' Rights and the Intellectual Property Dynamic in Agriculture' [2014] The SAGE Handbook of Intellectual Property 238.
[20] Jonge (n 14).
[21] International Union for the Protection of new Plant Varieties (UPON), 'Act of 1991 - International Convention for the Protection of New Varieties of Plants' (Retrieved from http://www.upov.int/upovlex/en/acts.html, 1991).

filing the application, or in a foreign country, earlier than four years; or six years in the case of trees or vines before the date on which protection is applied for[22]. The distinctness of a plant variety is the ability to clearly differentiate it from any other plant variety the existence of which is common knowledge before the time of application. The uniformity condition means that a plant variety must be sufficiently uniform in its characteristics. a plant variety is considered stable if its relevant characteristics remain unchanged after repeated propagation [23]. With respect to the scope of plant breeders' rights, the authorization of the plant breeder is required for various uses including the production or multiplication of the protected variety, for exporting and importing, and for its selling, marketing or offering for sale (UPOV, 1991, Article 14). With respect to the *exceptions* to the rights of plant breeders, the breeders' exemption allows protected varieties to be freely used for the purpose of breeding new varieties thereby allowing any breeder to have access to the latest improvements and new variation (UPOV, 1991, Article 15). The farmers' privilege, as included in the UPOV 1991 Act, is an optional exception that permits farmers to save and reuse seed of a protected variety on their own farm "within reasonable limits and subject to the safeguarding of the legitimate interests of the breeder" (UPOV, 1991, Article 15.2). With the farmers privilege, the African block PVP uses different variations suiting their situation. For instance, the SADC and ARIPO draft PVP laws employ different strategies to protect these "legitimate interests of the breeder": The ARIPO draft only provides a farmer's privilege for specific agricultural crops and vegetables with a history of seed-saving, which will be listed by the Administrative Council. Specifically excluded are fruits, ornamentals, other vegetables or forest trees (ARIPO, 2013a, Article 22.2). The SADC draft protocol uses the term 'subsistence farmers' to designate a specific category of farmers who alone are the beneficiary of the farmers' privilege (SADC, 2012, Article 27.d).

3. PVP IN AFRICA

Agriculture in Africa is an activity of primary importance. Most of the economically active workers in Africa are all from this sector and that agriculture remains an important economic activity. In Libya only, 7 percent of the population is engaged in agriculture, 92 percent of the population of Burkina Faso, 76 percent of the population of Kenya, 74 per cent of Senegal's population find employment in the primary sector and 54 percent Ghana labour force is engage in agriculture (FOA 1999). Further, agriculture's contribution to the GDP can be very substantial, reaching 26 percent in Kenya, 32 percent in Nigeria, 42 percent in Cameroon, 50 percent in Ethiopia and 54 percent in Ghana (New York 2000).

Seed management in African countries is largely carried out by farmers. Indeed, farm-saved seeds account for about 80 per cent of farmers' total seed requirements. These proportions are even higher in some cases (London 199), even when farmers buy seeds for the crops they market, they usually continue to cultivate local food crops (Centre for Development Research, 1999). Traditionally, agricultural management has been built around significant sharing of knowledge and resources

[22] ibid.
[23] ibid.

at all levels [24].

Most African countries are members of the World Trade Organization (WTO), which has established minimum standards of intellectual property (IP) protection for all its member states through the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) [25]. With respect to plant varieties, the TRIPS Agreement obliges members to provide for the protection of plant varieties either by patents or by an effective sui generis system, or by any combination thereof (TRIPS agreement 1994). In 2014, the regional IP organization of West Africa, the African Intellectual Property Organization (OAPI), joined UPOV as its fifth member in Africa. One year later, the African Regional Intellectual Property Organization (ARIPO) of mainly eastern and southern African countries adopted the Arusha Protocol for the Protection of New Varieties of Plants, which is largely in conformity with the UPOV 1991 Convention [26]. Other regional organizations, such as the South African Development Community (SADC), the Common Market for Eastern and Southern Africa (COMESA) and the East African Community (EAC) have planned to establish similar PVP systems [27]. Together, these regional organizations encompass most countries in sub-Saharan Africa.

By establishing such PVP systems, African countries hope to incentivize breeding and the introduction of new varieties, allowing farmers to access a wide range of improved varieties to contribute to both economic development and food security [28]. Yet, these developments are being strongly opposed by several civil society organizations (CSOs), which are of the opinion that, the proposed legal frameworks are unsuitable for most African countries. A key concern is that a UPOV-based PVP system merely favours the interests of commercial breeders and marginalizes smallholder farmers by impeding the traditional farming practices of using, exchanging and selling farm-saved seed (Saez, 2013).

This misunderstanding between proponents and opponents of the ongoing regional harmonization processes have taken centre stage and can be found both at the regional and national levels in Africa which has caused drawback to African breeders' ability to breed for different varieties to support changing environment. However, many smallholder farmers in Africa have difficulties in accessing quality seed of genetically superior varieties from these formal seed systems due to physical and financial constraints. These farmers may only access new varieties through the use and exchange of farm-saved seed. The challenge for African countries is to strike a balance between protecting the interests of breeders and maintain the incentive function of plant breeders' rights in the commercial market, while providing sufficient leeway to smallholder farmers that depend on informal

[24] Louwaars (n 6).

[25] World Trade Organisation (WTO), 'Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)' (Retrieved from http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm, 2015).

[26] African Rigional Intellectual Property Organization (ARIPO), 'Draft ARIPO Legal Framework for the Protection of New Varieties of Plants' (Retrieved from http://www.ip-watch.org/2013/11/28/critical-moment-for-africas-small-farmers-as-aripo-decides-on-plant-v ariety-protection/, 2013).

[27] Southern African Development Cooperation (SADC), 'Draft Protocol for the Protection of New Varieties of Plants (Plant Breeders' Rights) in the Southern African Development Community Region' (Retrieved from http://www.ip-watch.org/2013/04/05/african-regional-plant-variety-protection-draft-legislation-raises-protes t/, 2012).

[28] Zinatul A Zainol and others, 'Biopiracy and States' Sovereignty over Their Biological Resources' (2011) 10 African Journal of Biotechnology 12395.

sources for their seed security and survival.

In most African countries, PVP is relevant for only a small segment of the formal seed sector for instance, Kenya and Zimbabwe, which already have plant variety protection regimes in place. In both cases, the introduction of plant variety protection has not substantially fostered the development of new food crops. On the contrary, in Kenya, out of 136 applications filed and tested since 1997, only one was a food crop while most concerned were cash crops such as ornamentals or sugarcane and more than half concerned were rose varieties. A PVP system will not incentivize breeding in crops for which there is no commercial market. This implies that in many African countries a PVP system will only serve a minor share of the existing seed systems, most notably those that cater for the needs of large commercial farmers linked to national and international markets.

Most of the countries in Africa are still developing and it is in their best interest to seize or adopt a PVP system that suits their specific needs. Most of the system favours already developed countries. There are several examples of countries which/who? drafted alternative sui generis system for the protection of plant varieties, like Thailand and India. This will protect the rights Local Communities, Farmers and Breeders, and for the Regulation of Access to Biological Resources. One optional exemption in UPOV 1991 is the so-called 'farmers' privilege', which holds that countries may allow farmers to save and reuse seed of a protected variety "on their own holding" and "within reasonable limits and subject to the safeguarding of the legitimate interests of the breeder. This means that the exemption may only apply to a specific set of crops, and does not allow for any form of exchange of farm saved seed. In addition, farmers may need to remunerate the breeder for reusing seed of a protected variety. Taking in mind the breeders right should not be violated.

3.1. West Africa

Problems with limited availability, poor quality, and high prices of certified seeds and fertilizers are common in West Africa and represent a major barrier to agriculture growth. To improve the situation, West African governments have been working through ECOWAS and other regional bodies for several years to develop harmonized trade rules and quality control procedures designed to increase farmer choice, bring prices down, improve buyer confidence, and otherwise make input trade easier, faster, and cheaper. The lower yields of farmers in West Africa are contributed by unimproved seeds, including traditional landraces and seeds of improved varieties that have been recycled for so many years which no longer provide a yield advantage. Setimela *et al.* (2009) compared 2,007 adoption rates of improved maize varieties in 14 Sub-Saharan African countries and found that West Africa (represented by Benin, Ghana, Mali, and Nigeria in the sample) had the lowest adoption rates compared with other parts of Africa.

Apart from industrial cash crops where inputs are often provided by processing companies, most farmers in West Africa have little or no access to improved inputs for food staples. For food crops, farmers typically have to travel long distances to find improved seed and fertilizer and then face problems of little choice, high prices, and uncertain quality. Giving breeders in West Arica the right to own their varieties will encourage them to breed for crops to support the ever-changing

environmental conditions and soils in West Africa. Most of the francophone West African countries have already joined UPOV through the Francophone African Intellectual Property Organization (OAPI).

Other anglophone countries such as Ghana has joined UPOV whereas others are in touch with UPOV office with the intention of joining later. The main objective of the SADC and ARIPO draft PVP laws is to create a regional PVP system that is fully in tune with the highest international standard "to boost agricultural production and develop the agri-business value chain for economic growth" (ARIPO, 2012). This push for a harmonized PVP system has been met with much criticism. The CSOs essential claim is that such a 'one-size-fits-all' UPOV '91 based regime is unsuitable for the needs of individual member countries and their farmers, and does not consider the different levels of development among the member countries [29]

3.2. Ghana

Ghana as a country has passed out about six obligations in pieces of legislation in the area of intellectual property between 2003 and 2006.The legislation enacted includes Patents Act, 2003 (Act 657), Geographical Indications Act, 2003, (Act 659), Industrial Designs Act, 2003 (Act 660), Trademarks Act, 2004 (Act 664), Layout - Designs (Topographies) of Integrated Circuits Act, 2004 (Act 667) and the Copyright Act, 2005 (Act 690). These pieces of legislation created a new landscape for the regime of intellectual property but overlooked the development and protection of rights related to plant varieties [30]. The protection for new plant varieties is expected to encourage investment in plant breeding in the country since plant breeding requires long term investment and efforts which entrepreneurs are most often unprepared to sponsor in the absence of protection. Presence of a PVP act also promote agricultural development and to ensure food security[31]. In line with Government's effort to improve the seed industry, by stimulating competition among enterprises, encouraging price stabilisation and offering employment to the private sector, the Ministry of Food and Agriculture acknowledged the significance of plant variety protection as an important element of the country's national seed policy initiative [32]. For the country to increase its productivity per unit area, a lot depends on the quality of seeds planted. It therefore became critical that the country creates and promote an enabling environment for the stakeholders in the seed sector through the development of policies and strategies to ensure food security and increase the efforts of the country to compete on international markets, in addition to bringing about crop diversity and improvement to compete in the world market.

In complying with the TRIPS agreement, Ghana opted to develop a sui generis system for the protection of new plant varieties in line with the UPOV Convention

[29] (Jonge, 2014)

[30] Hans Adu-dapaah and Grace Issahaque, 'Becoming a UPOV Member: Ghana's Experience and PVP up Date' (The Asia and Pacific Seed Association (APSA), Singapore, 2021).

[31] HM Bortey and F Mpanju, 'Adoption of Plant Breeders' Rights System: Perceived Implication for Food, Seed Security and Sovereignty in Ghana' (2016) 21 Journal of Intellectual Property Rights 96; Adu-dapaah and Issahaque (n 30).

[32] Republic of Ghana, 'National Seed Policy' (http://semences.minagri.gov.rw/SIFSR/Data/11EN020I026v2.pdf, 2013) 123.

[33]. Ghana started its PVP bill preparation in the year 2000 and went through tussle and opposition from civil society organizations (CSOs) for a period of 20 years [34]. The bill was initially put on hold by Ghana parliament due to issues raised against the bill in a petition to the parliament of Ghana by CSOs [35].

Among others, the major concerns raised against the bill include the following: Clause 23 of the bill stipulates that "A plant breeders right shall be independent of any measure taken by the Republic to regulate within Ghana the production, certification and marketing of material of a variety or the importation or exportation of the material". The interpretation given of the clause was that the clause is seeking to prohibit the Government of Ghana from regulating the activities of the plant breeders as regards production, certification and marketing of material of a variety or the importation or exportation of the material. Secondly, clause 20 (6)c of the Bill stipulates that "an essentially derived variety may be obtained for example by the selection of a variant individual from a plant of the initial variety, backcrossing or transformation by genetic engineering".

The concern was to the effect that the clause is to provide an opportunity for the production of Genetically Modified Organism (GMOs). They argued that food variety in the country should be an origination of other existing variety which has been modified through selection and breeding. it should be free from genetically modified organism (GMO) because GMO food raises issues of food safety and its consumption has heath implications. Also, there was concern that the bill is based on the International Union for New Varieties of Plants (UPOV) Convention 1991, which favours industrial seed breeders that develop genetically uniform seeds/plant varieties suitable to mechanised large-scale agriculture. They suggested that passing the bill in its state would increase the activities of commercial seed breeders and increase the dependency of small-holder farmers on commercial seed varieties, forcing farmers to buy seed during each planting season [36]. They rather advocated for a *sui-generis* system that is more farmer friendly and would accommodate the rights of communities and associated indigenous knowledge, innovations, technologies and farming practices. The concerns of the CSOs were referred to the committee on constitutional, legal and parliamentary affairs for further deliberation.

The parliamentary committee in a meeting with the CSOs manged to convincingly addressed the issue that the bill makes provision for small-holder farmers to save seeds, as well as experiment them to develop new improved varieties. Also, it gives farmers the opportunity to develop their own variety and protect it [37]. On the concern of linking the PVP act to genetic modified organism (GMOs) bill, the parliamentary committee clarified to the CSOs and concerned citizens that, the Bio-Safety Act, 2011 (Act 831) takes care of research into GMO in the country and the safe and sustainable use and related matters and that the PVP bill focuses solely on promoting and protecting breeders, farmers and seed producers that develop genetically uniform seeds plant varieties suitable for

[33] Adu-dapaah and Issahaque (n 30).
[34] ibid.
[35] Parliament of Ghana, 'Report on the Petitions on the Plant Breeders Bill, 2013' (Parliament of Ghana, Accra Ghana, 2014) 24pp.
[36] ibid.
[37] ibid.

agriculture [38].

The parliamentary committee recommended an increased awareness raising campaign to engage major players who will directly and indirectly by the adoption and implementation of the bill specifically, basic key provisions of the bill should be explained to their understanding using effective media channels depending on the target audience [39]. The PVP bill was finally passed by Ghana's parliament in the year 2020 as the Plant Varieties Protection Act 2020 (Act 1050) [40] and gazetted on 29th of December 2020. Ghana eventually acceded to UPOV on November 4, 2021[41]. To operationalize the Act, Ghana is in preparation of the required legislative instruments to be passed by Parliament. Parliament has instructed that legislative instruments be developed and passed within one year of the passing of an Act by Parliament.

3.3. Uganda

Uganda passed its PVP Act in 2014. Like most other countries, the aim of Act is to provide for the promotion and development of new plant varieties and their protection as a means of enhancing breeder's innovations and rewards through granting plant breeder's rights. The act seems to be holistic and liaise with different aspects of seed regulation and policy. The Act grants different duties to different bodies in relation to the discovery, registration and implementation of the rights accorded to different breeders. Under the act, the Ministry of Agriculture, Animal Industry and Fisheries is responsible for the general PVP in Uganda. The Act indicates that the Minster has the duty to constitute the Plant Variety Protection Committee. The Minster also has the duty to make regulations for giving full effect to the provisions of the Act. Second is the Office of the Commissioner of Crop Inspection and Certification which is directly in charge of creating a register of all plant varieties in Uganda and updating the same. The office has the main responsibility of receiving and examining applications for the registration of plant breeder's rights and assigning the plant varieties for testing. This office is also tasked with the responsibility of publishing applications of the plant breeder's rights in the Gazette as well as any objections thereto.

Upon successful grant of the rights, the registration and later issue of the certificate is done by this office. Finally, the major duty of implementation and protection of plant breeder's rights is carried out by this same office. Also, there is a Registrar who is appointed by the minster and heads the office of the Commissioner of Crop Inspection and Certification office. The Ugandan PVP act has similar provisions as other national and regional PVP acts. The major criticism has been in allowing non-citizens to apply for protection. Whereas most PVP acts require foreigners to get representative residents to lead in the application in their jurisdiction, the Ugandan act allow non-residents direct application. Opponents have maintained that this very clause would open the flood gate for foreigner who

[38] ibid.

[39] HM Bortey and F Mpanju, 'Adoption of Plant Breeders ' Rights System : Perceived Implication for Food , Seed Security and Sovereignty in Ghana' (2016) 21 96.

[40] Republic of Ghana, 'Ghana's Plant Variety Protection Act 1050 (2020)' (Republic of Ghana, Accra, 2021) 1.

[41] Adu-dapaah and Issahaque (n 30).

have the financial power to flood the market with their varieties as the expense of the local nascent breeding institutions and companies. Application can be made in respect of a plant variety which is either bred locally in Uganda or outside Uganda[42].

3.4. Kenya

Reports indicate that Kenya is one of the leaders of PVP implementations on the African continent with over 500 rights granted. It has therefore been featured in most impact studies [43]. The legislation for protection of plant varieties in Kenya is contained in Seeds and Plant Varieties Act (1972), which became operational in 1975 and was revised in 1991 and amended in 2012. Official regulations to guide the implementation of Kenya's PVP were finalized and gazetted in the supplementary issue of the Seeds and Plant Varieties Act (Cap326) of November1994. The administrative office of the PVP was established in 1997 and has functioned under the Kenya Plant Health Inspectorate Service (KEPHIS) since 1998. Kenya acceded to UPOV under the 1978 Convention in May1999 and the1991 convention in May 2016 [44].

Impact studies indicate that the PVP system has encouraged investment and effort into plant breeding in Kenya especially in the cut flower industry. It allows Kenyans access to internationally bred varieties which would not be available to them without legal protection of these varieties. Other benefits also include farmers access to an increased number and range of improved varieties. Generation of foreign exchange and employment**.** Thus, breeders' rights therefore benefit not only the breeders, but also the public in general [45]. Although foreign horticultural industry pressed for the establishment of PVP in Kenya, the national regime has added confidence and contribute to the perception of a better business environment for expansion. industry.

4. PVP, INTELLECTUAL PROPERTY AND THE AFRICAN CONTINENTAL FREE TRADE AREA

The African Continental Free Trade Area (AfCFTA) seeks to establish a single continental market where goods, services and people can move easily, and to effectively expand intra-African trade across the continent. The object is to enhance competitiveness and support economic transformation of Africa. The Pact covers trade in goods and services, investment, intellectual property rights, as well as competition policy[46]. The Phase II of the treaty holds many opportunities,

[42] Dimuth Siritunga and others, 'Impacts of Strengthened Intellectual Property Rights Regimes on the Plant Breeding Industry in Developing Countries: A Synthesis of Five Case Studies', *Impacts of Strengthened Intellectual Property Rights Regimes on the Plant Breeding Industry in Developing Countries: A Synthesis of Five Case Studies* (9th ICABR International Conference on Agricultural Biotectnology Ravallo, Italy, July 6 to July 10, 2005 2005).
[43] Bortey and Mpanju (n 39); Jonge (n 14); Siritunga and others (n 42).
[44] Simon K Kibet, 'Impact of Plant Variety Protection in Kenya', *Seminar on "The benefits of the UPOV System of Plant Variety Protection for farmers and growers* (UPOV, Swizerlanad 2017).
[45] ibid.
[46] Ncube (n 12).

particularly for Intellectual Property (IP) including plant variety protection (PVP). Intellectual property rights are said to be territorial in nature, which implies that national laws regulate the conditions for their acquisition, maintenance and enforcement. In its quest to the attainment of a single continental market, Article 4 of the AfCFTA Agreement proposes the cooperation of state parties on investment**,** intellectual property rights and competition policy. Secondly, it encourages leveraging the IP protocols on already existing regional IP regimes, such as those of those of ARIPO and OAPI, in order to streamline the continent's IP policies [47].

Apart from the general provisions on co-operation by member states, the IP Protocol should also focus on IP regimes that are not sufficiently exploited in Africa, which includes geographical indications, plant variety protection, protection of genetic resources, traditional knowledge and other cultural expressions. For example, Africa's agricultural products typically have qualities that derive from their place of production and are influenced by specific local geographical factors. Such products could be protected with geographical indication (GI). One of the real-world benefits of plant variety protection is to encourage the development of new, improved plant varieties that lead to improved competitiveness in foreign markets. To achieve this, the PVP regime of the continent would need to be strengthened.

With cognizance to the IP harmonization plan of the AfCFTA, the continental PVP regime would a unified PVP like that of ARIPO and SADC PVP legislations [48]. Such regime would provide a 'one stop shop' approach whereby a single protection title will cover all contracting parties, reducing costs and administrative hurdles for breeders, allowing varieties to be available in more countries, and facilitating effective synergies in the (technical) operations of national systems. However, there has been a lot of criticism against such a harmonized PVP system. Opponents claim is that such a 'one-size-fits-all' UPOV '91 based regime is unsuitable for the needs of individual member countries and their farmers, and does not consider the different levels of development among the member countries [49]

5. PROSPECTS AND CHALLENGES FOR PVP IN AFRICA

Many African countries have in ready a plant variety protection (PVP) bill awaiting implementation or have acceded to a regional PVP act [50]. Proponents of stronger plant breeders right (PBRs) argue that it will enhance farmers' and growers' access to wide range of improved plant varieties. They also contend that it will encourage plant breeding research and development and overall advancement of agricultural production. The anticipated collective effects are reported to include the enhancement of national and regional economic development, improvement in food security and sustainable agricultural production in Africa [51].

[47] ibid.
[48] Philippe Cullet (n 10).
[49] Jonge (n 14).
[50] Oguamanam (n 5); Jonge (n 14).
[51] Oguamanam (n 5).

Few African countries have gone past a draft PVP bill to implementation. Studies on the impact of plant breeders' rights (PBRs) in Africa regarding the above expectations is quite contentious and divergent [52]. The overall effects of plant intellectual property in developing countries are difficult to discern conclusively and researchers find themselves having to rely on the experiences of developed countries". Concerns have also been raised about the design and sponsors of such studies in the developing world [53] . Kenya, Tanzania and South Africa are the key African countries that have advanced in their PVP implementations and are often used as representative countries for impact studies in Africa [54]. In Kenya and South Africa, it was reported that the number of resident breeders who applied for PBR increased in from 1997 to 2003 with the introduction of a PVP system.

With that, even though there was appreciable increase in the number of food crops, most of the crop's protection was sort for were ornamentals[55]. Some authors therefore argue that a PVP system encourages the protection of non-food crops and there is the likelihood of shifting breeding attention to these crops at the expense of food crops which will have dire consequences to food and nutritional security on the continent. Others also are of the view that, ornamental plants are equally potential source of income into an economy and contributes to the gross domestic product through foreign exchange [56].

As already noted, the practical realities of agricultural production in developed countries are in sharp contrast to developing countries, especially in African. The African agriculture possess a unique long-observed practices and traditions unlike the developed world [57]. It characterized by a sense of communism, hence sharing and exchange of resources like seeds and planting materials is a recognized tradition. As a result, any system that seeks to change this long-held tradition would be fiercely confronted with a high sense of doubt.

Opposition to Africa embracing the UPOV based PBRs has come in gushes from diverse stakeholders, notably, civil society organizations, farmers' rights groups, development NGOs, food security, biodiversity conservation and traditional knowledge experts. They are of the view that, the UPOV-style PBR is not suitable for a smallholder farmer-centred agrarian system that is prevalent on the African continent. It turns to favour only breeders at the expense of farmers. It does not consider the containment of farmers' practice to freely exchange of farm-saved seeds. This is evident in the revision of the UPOV convention from1972,

[52] Robert Tripp, Niels Louwaars and Derek Eaton, 'Plant Variety Protection in Developing Countries. A Report from the Field' (2007) 32 Food Policy 354.
[53] Jeroen van Wijk, 'How Does Stronger Protection of Interllectual Property Rights Affect Seed Supply? Early Evidence of Impact' [1996] Natural Resources Perspectives 1; Oguamanam (n 5).
[54] Bortey and Mpanju (n 31).
[55] (De Jonge, 2014)
[56] Karine Peschard, 'Seed Wars and Farmers' Rights: Comparative Perspectives from Brazil and India' (2017) 44 Journal of Peasant Studies 144 <http://dx.doi.org/10.1080/03066150.2016.1191471>; Bongo C Adi, 'Intellectual Property Rights in Biotechnology and the Fate of Poor Farmers' Agriculture' (2005) 9 SSRN Electronic Journal 91; Biswajit Dhar and Sachin Chaturvedi, 'Introducing Plant Breeders' Rights in India' (2005) 1 The Journal of World Intellectual Property 245; Tilahun Weldie Hindeya, 'TRIPS, Plant Varieties and the Right to Food: A Case Study of Ethiopia's Legal Regime on Protection of Plant Varieties' [2014] SSRN Electronic Journal 77; Bortey and Mpanju (n 31).
[57] (De Jonge, 2014)

1978 and to 1991. Each revision marks a progressive shrinkage of grudging accommodation of farmers' privilege to use farm saved seeds and increase in the scope of breeders' rights, including rights to share seeds amongst themselves [58].

Opponents of stronger PBR have based their argument mainly on farmers rights; a concept that was introduced when it was realized that the established IPR regime did not recognised farmers as innovators and disqualified them from holding IPRs. The introduction of farmers' rights is to enable share benefit arising from genetic resources, and to give farmers initiative to preserve their genetic resource and share them with others.

Most relevant international legal instruments on agriculture and farming such as the Convention on Biological Diversity [59], Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization [60] and the International Treaty on Plant Genetic Resources for Food and Agriculture [61] make a link between biodiversity conservation, traditional knowledge in the use of genetic resources and the need for access and benefit sharing as between users and custodians of genetic resources [62]. Within the matrix of these instruments, traditional knowledge of uses of genetic resources, which includes traditional agricultural and farming practices are recognized as crucial aspects of innovation.

An attempt to downplay the importance of farmers as crucial part of breeding innovation with little or no rights is unfair and effort to separate breeding from farming in Africa would be a very challenging one [63]. Opponents of Africa's adoption of the UPOV-PBRs framework recommends linking any sui generis system for protection of plant varieties to systems that protect communities' rights, indigenous and bio-cultural knowledge and practices. Stronger PVP regime which ignores such link would be considered out of agreement with international rules [64].

The UPOV-PBRs system is considered highly breeder-centred and fails for fitness for purpose regarding the reality of agriculture production in Africa. Despite the farmer-centred nature of African agriculture, there is marginal mention or accommodation of farmers alongside the expansive scope of breeders' rights under the UPOV's system. The scope of the UPOV 1991 breeders' rights include exporting, importing, offering for sale, conditioning, stocking for propagation purposes and overall commercial exploitation of the protected varieties. Also, whereas breeders are free to deal with protected variety for experimentation purposes, farmers are not allowed to commercially exploit those varieties save on terms prescribed by breeders. Whereas breeders could conceptually have unregulated access to farmer varieties, even to the extent of potentially exercising proprietary interests over materials essentially derived there from, farmers are not

[58] Oguamanam (n 5).
[59] United Nations (UN), 'Convention on Biological Diversity (CBD).' (Retrieved from http://www.cbd.int/convention/text/, 1992).
[60] United Nations (UN), 'Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from Their Utilisation to the Convention on Biological Diversity' (Retrieved from http://www.cbd.int/abs/text/, 2010).
[61] Food and Agricultural Orgainization (FAO), 'International Treaty on Plant Genetic Resources for Food and Agriculture (ITPGRFA).' (Retrieved from http://www.planttreaty.org/content/texts-treaty-official-versions, 2001).
[62] Oguamanam (n 5).
[63] Jonge (n 14).
[64] Oguamanam (n 5); Zainol and others (n 28); Adi (n 56).

allowed to commercially exploit breeders' protected varieties in the same manner [65].

Concerns have also been raised about the farmer-unfriendly and discriminating nature the criteria for protection enshrined in some of the regional draft PVP legislation (ARIPO and SADC) emanating from the UPOV 1991 act. The CSOs question the appropriateness of the criteria of novelty, distinctness, uniformity and stability (NDUS) in Sub-Saharan Africa PVP bills for several reasons: (1) the novelty requirement is exclusively focusing on commercial novelty; (2) the criteria for distinctness contains a very low threshold for inventiveness; (3)the uniformity standard will lead to erosion of genetic diversity and, thus, increasing genetic vulnerability; and (4) the uniformity and stability requirements makes it very difficult for farmer varieties to be eligible for protection [66]. One recommendation has been to replace the UPOV standards of uniformity and stability by 'identifiability', i.e., by describing a typical combination of characteristics of the new plant variety in order to fulfil the legal need to identify the protected subject matter without prescribing the physical properties a plant variety needs to have [67]. This approach would make it possible to have protection of plant varieties or groupings that are more heterogeneous and variable, like landraces and farmer varieties. Such varieties are deemed very important for food security because of their heterogeneous and unstable characteristics that fit local agro-ecological conditions and can respond to changing conditions in the face of climate change.[68]

Lastly, considering the paucity of local plant breeding activities in Africa, opponents are of the view that, a stringent PVP framework like the UPOV based would prepare the grounds for foreign seed companies to flood the African market with their products at the expense of development of local breeding programs and institutions. There is also the possibility that, most of the crops that would obtain breeding investment and protected varieties may not be food crops which could go on to worsen the food and nutritional security of the continent [69].

CONCLUSION

While protection of plant varieties is mandatory under TRIPS, the agreement gives member countries substantial flexibility in this regard. Not only does Article 27(3) permits selection of the means of protection (patents, a sui generis system or a combination of both) but it also allows individual countries to choose a sui generis system and define for themselves the components of such system. The only requirement is that the system be "effective," which means that, at the very least, it

[65] Oguamanam (n 5).
[66] (De Jonge, 2014)
[67] Campi (n 7).
[68] Peschard (n 56); UPOV, *Guidelines for the Conduct of Test for Distinctiness, Uniformity and Stability of Rice* (Internationa Union for the Protection of New Varieties of Plants, Geneva, 2004); De Jonge (n 29); V Mathur and P Musyuni, 'Plant Variety Protection Legislation: Overview of an Indian and African Perspective' (2018) 2 International Journal of Drug Regulatory Affairs 12.
[69] Civil Society Organizations (CSOs), 'Civil Society Concerned with ARIPO's Draft Regional Policy and Legal Framework for Plant Variety Protection.' (Retrieved from http://www.acbio.org.za/index.php/media/64-media-releases/409-aripospvp-law-undermines-farmers-rightsa- food-security-in-africa, 2012).

provides for an intellectual property right. However, many African countries have opted for the UPOV based plant variety protection system. There has been widespread criticism and oppositions from farmer groups, civil society organizations and diverse stakeholders in Africa against such a strong UPOV based PVP system for Africa. Proponents of a PVP regime have outlined a number of benefits Africa's agriculture stands to gain in adopting a PVP system. Opponents have also put out the possible threats of a strong PVP system could pose to Africa's agriculture. Notwithstanding, many countries have opted for it and have draft PVP bills awaiting implementation. Whether Africa stands to gain from a PVP regime or not, only time will tell.