ISSN (online) 2664-9535 (print) 2664-9527 https://atcr.kra.go.ke

Digital Taxation in Tackling Illicit Financial Flow in Developing Countries

Ndirangu Ngunjiri [1]

[1] Watermark Consultants Ltd, Nairobi, Kenya

Received 18 March 2022
Accepted for publication 05 April 2022
Published 19 April 2022

Abstract

Illicit financial flows not limited to crime, corruption, and tax evasion are an increasing concern all over the world. Among the targets in Sustainable Development Goals (SDGs) is stemming the flow of illicit funds. However, there exists no consensus on the accurate definition of illicit financial flows or how to measure them. Some argue for the definition to cover illegal behavior such as tax fraud and evasion as well as legal behavior that reduces tax revenue. To curb illicit financial flows, the use of digital technologies has emerged as one of the preferred methods among other ways such as closing loopholes in tax treaties. This will help countries mobilize funds for efforts including poverty reduction. This project aims to establish how digital taxation has helped countries curb the flow of illicit finance. The existence of vulnerable financial systems contributes to reduced tax revenue leading to constrained social and economic development. Collaboration among the various arms of government is among the research's policy recommendations. The policies should aim at strengthening institutions to enhance rule of law, meeting contractual obligations, and property rights protections in the jurisdictions. The countries should actively seek to strengthen international financial and technical cooperation to combat illicit financial flows (IFFs).

Keywords: Illicit, Taxation, Technology, Evasion, Countries

1. Background

Digital tax implies a tax levied on income from the digital marketplace. A digital marketplace is a platform that enables direct interaction between buyers and sellers of goods and services through electronic means. IFFs are brought about by; mis-invoicing, illicit goods, transfer pricing, corruption, and trafficking of humans. In Kenya, the digital tax was introduced by the Finance Act 2020. The relevant authorities such as the cabinet secretary in charge of finance reiterated the many challenges posed by a fast-evolving digital economy. Among the challenges noted are the economy's overreliance on intangibles, determining jurisdiction value, massive utilization of data, and adoption of multi-sided business models. The challenges led to tax base erosion leading to low tax revenue. The introduction of the digital tax was meant to address these challenges by expanding the tax base by netting the digital economy, which may not necessarily have a physical presence in the jurisdiction in Kenya, a resident and non-resident person are taxed based on their presence in the country. Even before the introduction of a digital tax, taxation was already covered in the income tax legislation. According to the Act, a digital marketplace is any platform that allows the buyer and the

seller to interact electronically. The introduction of digital tax was meant to remove any ambiguity in the administration. The digital services tax (DTS) charges 1.5 percent of the gross transactional value of any income earned through the digital marketplace.

According to research done by the Partnership for African Social and Governance Research (PASGR) in 2018, illicit financial flows are a persistent problem in developing countries. The problem is especially worse among sub-Saharan countries accounting for the huge sum of funds shifted out of the jurisdictions. Resources that could otherwise finance much-needed development in public services. The research postulates that Kenya lost approximately KES 40 billion annually since 2011 due to illicit financial flows. The problem is not limited to multinationals, but also local firms and governments.

In developing countries, illicit financial flows occur mostly through mis-invoicing, dealing in contraband goods, transfer pricing, corruption, and human and drug trafficking. The vice takes many forms not limited to grand corruption scandals such as the transfer of illicit funds by the political class since independence. To facilitate IFFs, officials from key government agencies such as the police, military, and tax collecting authority are usually perpetrators. Another important group is multinational corporations (MNCs), which engage in transfer pricing, avoiding income tax through mis-invoicing, and being overly being financed by debt from parent companies such that they incur interest on loan repayments, which is tax-deductible. A good example of this is parent flower companies in the Netherlands making huge profits contributing $250 million to the economy, but their subsidiaries in Kenya incurring massive losses. Introduction of digital taxation. Which targets universal registration of local and foreign firms will ensure Kenya does not lose vital revenue through tax evasion. All employees of foreign firms should appear in digital systems such as KRA's iTax platform.

Problem Statement

Developing nations especially those in sub-Saharan Africa have been losing a lot of revenue through illicit financial flows. Resources that could otherwise be pivotal in improving public services such as security, education, health, and many other much-needed developmental areas. The Global Financial Integrity Research Institute defines IFFs as the cross-border earning, transfer, and utilization of illegally earned funds. The current research will review published and grey literature to explore how digital taxation can help curb illicit financial flows in developing nations. Every year funds flow out of developing countries illegally. This weakens financial systems limiting their economic potential. The practice is occurring in all countries but is severe in developing countries considering their smaller resource base and markets.

Introducing a digital services tax is a means of actively strengthening international financial and technical cooperation to combat illegal financial flows through reforming fiscal systems. Globalization has brought to the fore the significance of IFFs. There is difficulty measuring the exact IFFs flowing out of developing countries more than donor assistance from OECD countries. In Sub-Saharan countries. It's a persistent problem given their small resource base. Therefore, the big question is do digital technologies facilitate illicit financial flows? They facilitate illicit financial flows at each stage be it earning, transferring, or using money illegally. Digital technologies facilitate the migration of traditional organized crime in addition to facilitating underground illegal markets of cybercrime and related crimes. Digital technologies provide opportunities for fraud, tax evasion, corruption, tax evasion, and other criminal activities. New digital tools for transferring money such as mobile banking, online banking, electronic payments, cryptocurrencies, online gambling services, and e-commerce providers have provided easy platforms for transferring and use of illicit money. They provide countless ways for perpetrators to distance money from illegal sources of profit or means to transfer it illegally from legal sources. They facilitate the transfer of illegal profits and aggregation of the funds in offshore accounts. They allow for the placement of illicit funds in fake e-commerce companies and offshore online enterprises.

Despite all the challenges experienced with digital technologies, they offer avenues for tackling illicit financial flows. They can serve as a tool for empowerment and transparency, which can be used in investigations, detection, and disruption of the transfer of illegally earned money. The tools complement but do not substitute legal frameworks such as instituting digital tax, international cooperation, and public-private collaborations. Technological measures help in the implementation of complex mechanisms including legal and organizational components however, the use of digital technologies in the investigation should be balanced with human rights and personal privacy.

Purpose of the Study

This project aims to establish how digital taxation has helped developing countries, especially Sub-Saharan countries curb the flow of illicit finance, which is eroding much-needed revenue for public services such as education, security, health, and other social and justice services.

Research Questions

Do digital technologies facilitate illicit financial flows?

Does the introduction of digital taxation reduce the flow of illicit financial flows?

Significance of the study

The research study is significant in improving the livelihoods of people in developing countries. The research is important to various stakeholders including policymakers and

other interested parties. The study investigated the influence of using digital taxation on tax revenues collected by developing countries. The study hoped to assist developing countries to address challenges in dealing with IFFs. This will help them know how well to embrace technology in tackling the problem. Further, it is also hoped that the study shall contribute to the existing literature on the use of technology to empower tax administration authorities. The recommendations made will contribute to enhanced tax collection capabilities and socio-economic outcomes. It is hoped that this study will not only help in curbing IFFs but also cultivate the economic empowerment of the greater population.

2. Literature Review

The use of the term "illicit financial flows" is a relatively new concept (World Bank, 2016). The phrase described disconnected issues relating to tools, activities, and methods used by criminals to move funds and assets across national borders fraudulently. OECD, 2013. UNECA (2015) determines there is consensus in defining illicit financial flows as money earned, transferred, and used illegally.

However, the lack of consensus sets in when we look at studies debating the sources of illicit financial flows. Researchers agree that it should cover money earned through criminal activities or that earned legally but utilized illegally. Most of the literature lists several sources of illegal funds including crime, corruption, and illegal commercial practices.

Jansky (2013) splits illicit financial flows into groups: criminal flows, illegal corporate flows, and individual illicit flows. Other studies view the problem through the negative impact it creates rather than the activities. Blankenburg and Kahn (2012) consider financial transactions harming a country's economy as part of illicit financial flows creating a vague and broad definition covering many activities some on the borderline between legal and illegal.

Most debate on illicit financial flows focuses on where the line of determining between legal and illicit flows. One of such contentious debates is whether tax avoidance should be part of the definition. A report by the High-Level Panel on Illicit Financial Flows from Africa (UNECA, 2016) includes activities that while not strictly illegal in all cases are against norms and rules such as tax avoidance. Business practices that lower tax liabilities legally have elicited much debate due to concerns about including them in IFFs' definition. Inclusion is advocated by some states and civil society organizations while global financial centers favor a restrictive definition including corruption and crime but not tax planning to lower tax obligations if it does seriously and deliberately breach a jurisdiction's laws. Countries have different tax regulations providing opportunities for reducing tax liability. There is a need to address the issue of tax reduction in each country's context, however, that falls out of the scope of this research which focuses on how digital taxation can help stem the flow of illicit funds.

Despite the limited research on these fields, there is recognition of a link between digital technologies and illicit financial flows. However, the effect of information technology on sources of illicit profits is uneven.

Digital technologies: Crime as service for traditional organized crime groups

As reported by Euromix (2015), traditional crime groups had already started using digital technologies as "crime as service," hiring sophisticated cybercriminals to facilitate illegal operations. For example, in June 2013, law enforcement agencies in Belgium and the Netherlands took down a Netherlands-based drug smuggling ring, which employed hackers to penetrate the systems controlling the movement and location of shipping containers at the Belgian port of Antwerp. This infiltration involved interference with computer data to allow the criminals to remove shipping containers with drugs before the legitimate carrier could collect them. There are still relatively few known cases of such sophisticated manipulations with digital technologies in facilitating traditional criminal operations. However, they illustrate very well the potential scale of this problem.

Digital technologies and challenges of the digital economy

It is unclear to what extent digital technologies can facilitate illegal attempts to evade tax payments. Though it is hard to assume that the development of global communication networks does not affect tax evasion at all, it would be speculative to say there are many known distinct tools to illegally avoid taxes in the use of digital technologies. Of course, the global digital economy and the borderless internet create loopholes in the taxation frameworks, blur the line between illegal tax evasion and legal practices of tax avoidance, and pose particular challenges for tackling illegal activities. This area of research has emerged recently on the agenda of international organizations, such as the Organization for Economic Co-operation and Development (OECD 2014), which are currently undertaking studies and developing action plans concerning the problems of taxation in the era of digital technologies. Though the OECD admitted that severe erosion of tax bases could occur in the digital economy (OECD 2014), there is still no debate about the attribution of this problem to the use of particular technologies or specific behavior.

Illegal Online Marketplaces: Silk Road and Agora

One of the most infamous examples of hidden online marketplaces is Silk Road, which functioned similarly to legal auctions such as eBay, allowing "customers" to buy illicit drugs and other illegal commodities. It has been estimated that from 2011 to 2013, Silk Road facilitated over US$1.2 billion worth of sales between 4,000 vendors and 150,000 customers. The marketplace was shut down by the FBI (U.S. Federal Bureau of Investigation) in October 2013 but reappeared

shortly after as Silk Road 2.0 to continue criminal trade, until it was hit again in the Operation Onymous, which represented cooperation between law enforcement in the European Union and the United States, in October 2014. The closure of the Silk Road, however, has not stopped the further evolution of illegal marketplaces. The online marketplace, Agora, launched in 2013, surpassed Silk Road in the illegal drug trade and was named "the largest online narcotics emporium in the world" (Bertrand, 2015) one year after it was established. It has been estimated that Agora, as a platform for the trade of drugs, weapons, and illegal services, became the biggest black market operating online.

There is little doubt that complex tax fraud and tax scam schemes can rely on the use of digital technologies. However, while technology can play a certain role as an enabler of illegal activity, the main challenges are the globalization of the economy itself, the creation of digital multinational giants, and the possibility that digital technologies provide for the practice of "tax shopping," making it easier for companies to provide services without a physical presence and to look for the best place for establishing their headquarters and moving their profits.

Interconnection fraud and tax evasion in the telecommunications sector

The only known practice of tax evasion that is statistically proven and distinctly linked to communication technologies is the so-called "SIM box fraud" or "interconnect fraud, a type of manipulation that employs the internet to avoid call termination charges and, thus, revenue taxation. This scheme is a common practice in developing countries. It uses the voice-over-internet protocol to channel international calls away from mobile network operators and deliver them as local calls. In this case, the international call appears to be local and cannot be subject to significant international terminating charges. The same technique can be used to make local out-of-network calls appear to be handled within the network and, again, avoid termination charges (Ghosh, 2012).

Furthermore, when the government levies taxes on international calls, the operators themselves can use this scheme for diverting international calls, transforming them into local calls, and making fake declarations of incoming international call minutes to reduce the tax payable to the government (UNECA, 2015). This scheme especially affects developing countries in particular, on the African continent.

Interconnection Fraud: A Growing Problem for African Countries, Estimated Losses

In March 2015, Uganda's Financial Intelligence Authority started investigating suspected money laundering, revenue diversion, and tax evasion in the telecommunications sector, which could amount to US$144 million in lost revenue. The Ugandan Financial Intelligence Authority claims that the government loses as much as 45 percent in tax revenue, while the telecommunication operators lose more than 80 percent of their revenue (Reuters, 2015). A report from the High-Level Panel on Illicit Financial Flows from Africa states that the massive growth of the mobile industry brought significant losses in potential tax revenues because of the use of interconnection fraud. The report estimates losses in taxable revenue in Kenya as US$440,000 and refers also to the estimates of the Governments of Ghana (US$5.8 million in stolen taxes) and the Democratic Republic of Congo (US$90 million in tax revenue losses a year) (UNECA, 2015).

Digital technologies: A sure enabler of illegal money transfers

Transfers of illegal funds and money laundering have been dramatically influenced by the development of information and communications networks. Digital technologies offer countless opportunities to facilitate each traditional stage of illegal money transfer on their way to being distanced from illegal sources, which are placement, layering, and integration. Initially, the problem of money laundering with the use of digital technologies was mostly associated with the underground economy of cybercrime. However, as the payment systems are becoming more complex, decentralized, and dependent on the information networks, criminals can enjoy the opportunities digital technologies offer to transfer any type of illicit funds.

Technology does not care about the source of illegal income

While criminals can use different techniques and ways to gain ill-gotten profits, the tools that digital networks offer for distancing this capital from illegal activity are the same for any "dirty" money. The only difference between online and offline criminal activity is that money gained from cybercrime usually exists in cyberspace and has to be further transferred into cash and distanced from its source, so the placement stage of money laundering would be missing (Filipkowski, 2008). However, this can also happen with the illegal trade of goods online in digital currencies; money in this case is "pre-laundered" because it is placed in an unregulated financial institution (National Drug Intelligence Center 2008).

Information and communication networks as a game-changer for money laundering

Digital technologies have several unique features that make them a game-changer for money laundering:

Automation, speed, and their cross-border nature

The main advantages of global information networks are ease of use, speed of information transfers, automation, their cross-border nature, and the ability to operate in different jurisdictions without Placement are depositing money into the financial system, layering is distancing money from its source through a series of transactions, and integration is the commingling of money with funds in legal sectors.

Go Digital Technologies and Embezzlement/Corruption Schemes in Developing Countries

One of the biggest concerns concerning illicit financial flows is the possibility of siphoning money, especially foreign aid funds, in developing countries, through embezzlement and

money laundering. Millions of dollars are diverted from poverty-stricken nations through “phantom” firms and wire transfers to the bank accounts and companies in industrialized countries. For example, ONE, an international campaigning and advocacy organization, estimates that “at least $1 trillion is being taken out of developing countries each year through a web of corrupt activity that involves shady deals for natural resources, the use of anonymous shell companies, money laundering, and illegal tax evasion" (ONE, 2014). Though this might be an overestimate, certainly the funds flying out of the developing countries constitute very large sums. The question of how digital technology can facilitate this process is complex. In general, digital technology will enable any complicated money transfers, independently of the source thus, it can be used to slice down the money and transfer it through a combination of bank and e-payment transactions to aggregate illegal funds in a safe jurisdiction or integrate the money into the legal sector. However, the nexus of digital technology and corruption/embezzlement is much more complex than can be narrowed down to electronic money transfers only. Digital technology is not the only factor that can contribute to the complexity of transactions; it is the whole combination of such factors as cross-border trade, speed of communications, and the possibility of opening anonymous phantom companies without presenting identification documents or even without a physical presence. Establishing shell companies in some jurisdictions requires less information than obtaining a driver’s license or opening a bank account (ONE, 2014). These complex schemes might rely on information and communications technologies, but there is a lack of research and of evidence concerning the role that digital transactions can play in those intricate corruption and embezzlement models. There is little doubt that any tools for digital transfers analyzed in this chapter can be employed as a part of these schemes. However, further research and case studies are needed to investigate the nexus of digital technologies and complex schemes used to siphon money from developing states.

Anonymity

The absence of face-to-face transactions, which makes it difficult to implement know-your-customer techniques or monitor the behavioral patterns of the customers (FATF, 2008), is another key enabler of money-laundering schemes. Furthermore, many of the payment tools do not implement this technique at all and allow customers to enjoy full anonymity. Anonymity, in general, eroded the old models of traditional financial systems, which were usually based on long-term relationships with customers; unregulated online payment gateways nowadays provide the possibility for occasional transitions and transfers of micropayments (Council of Europe 2012).y

The complexity of online transactions

The complexity of the ecosystem of online transactions can be attributed to the rise of new payment intermediaries. These intermediaries follow different rules and allow for various activities; many payment providers permit transfers from one intermediary to another, some online payment platforms authorize peer-to-peer transfers, and several payment systems are connected to the traditional banking system and allow credit accounts with bank cards.

Implementation of the traditional techniques to monitor suspicious transactions by the payment providers can be undermined by the lack of implementation of these tools by other intermediaries or by the insufficiency of the information about client behavior (Council of Europe, 2012).

Lessor no regulation

Most of the intermediaries operating online are either less regulated than traditional financial institutions or not regulated at all (FATF, 2008). Anti-money-laundering measures that were implemented to fight illicit transfers fail when it comes to most digital payment providers.

Moreover, a payment intermediary can always benefit from the differences in regulation between various jurisdictions and choose a less regulated environment while being able to operate all over the world through global information networks. The aforementioned characteristics of digital technologies and online payment systems combined with the development of the information and communications networks allow criminals to combine different means for distancing ill-gotten money from the source of illegal profits. Several tools are mostly associated with money laundering in cyberspace: banking products and services, which to a large degree include regulated intermediaries; electronic payment systems via non-bank intermediaries; digital currencies, which are mostly unregulated and can also be decentralized; online services and trading platforms; online gambling; and e-commerce. These new tools can be combined with traditional methods of money laundering, thus creating a complex online and offline chain of multiple transactions, which are hard to trace and monitor, especially when they involve several jurisdictions. The following analysis provides insights into the way digital technology can facilitate transfers of illicit funds.

Online banking

Online banking is one of the most well-known nexuses of technology and money transfers, both legal and illegal. This link also represents the connection between technology and illegal ways to earn money. Banks and their customers are still one of the major targets for profit-driven criminals. Thus, in many cases, at the beginning of the process of illegal transfers, offenders are still dependent on the online transfers from or via regulated financial intermediaries, though frequently it can be combined with other tools (Council of Europe, 2012). Since regulated financial intermediaries carry out know-your-customer procedures and enter a business relationship with

customers before online banking can be used, criminals need to employ more complex schemes than just transferring funds using online banking. This is why, for example, when money is stolen from bank accounts with the use of digital technologies, cybercriminals face a certain bottleneck; to distance this illegal profit, they need money mules for online transactions, and money mules are a scarce resource. This is why criminals are searching for ways to avoid the use of mules and try, for example, to split the money into small amounts below the reporting threshold (Thomason, 2009) and move them quickly from and to different bank accounts between different financial institutions (Weaver 2005). This is where the benefits of digital technologies and automation are fully exploited. Some studies reveal that money launderers can carry out "hundreds of meaningless transactions across various bank accounts, followed by a limited number of cash withdrawals" (Council of Europe 2012). The possibility of performing many transactions through different institutions in various jurisdictions then makes it difficult, if not impossible, to detect illegal financial flows and trace them back (Malhotra, 2010).

Mobile banking and mobile payments

Mobile banking is a way of carrying payments via mobile phone with the use of different protocols such as text or the internet. In the process of mobile banking communication, operators act as financial intermediaries for handling the payment between a client and a business or financial institution (Filipkowski, 2008). Mobile communications operators, though subject to telecom regulation, are usually not opposed to the obligation to perform anti-money-laundering checks. The main driver for the evolvement of mobile banking is the growing demand for micropayments, especially in developing countries. The main vulnerability associated with the risk of the use of mobile banking for money laundering in many jurisdictions is the possibility of buying a pay-as-you-go SIM-card without registration and identity checks, and, thus, a great degree of anonymity, from which money launderers can benefit (Villasenor et al., 2011). However, the potential scope of using mobile banking for illegal transfers is debatable, because most of the transfers involve very small amounts of money. Although mobile payments are frequently named in different studies as one of the possible sources of digital money laundering, the latest reports produced rather controversial results and questioned the role of mobile banking in illicit financial flows. For example, a recent report from the Overseas Development Institute on capital flight in African countries concluded that although "in principle, mobile banking is likely to facilitate capital flight, especially the movement of illegal funds abroad…data on mobile money in Africa, however, seem not to confirm this hypothesis since no clear correlation can be identified between capital flight and mobile banking" (Massa, 2014). The report, however, still highlighted the vulnerabilities of online banking concerning illegal funds transfer and its potential for being used for money laundering.

Electronic payments via nonbank intermediaries

Online nonbank payment services provide a cheap, quick, and anonymous way to make international money transfers or to pay for goods and services. Unlike regulated financial institutions such as banks, these intermediaries are not subject to anti-money laundering obligations and thus do not have to perform checks on their customers or detect suspiciously money transfers. While the biggest online payment service providers, such as PayPal, developed anti-money-laundering policies and are trying to trace suspicious transactions, there are still many such intermediaries who allow criminals to enjoy the freedom of money transfers with no checks. Furthermore, some of the services allow peer-to-peer money transfers, making monitoring of suspicious activities even harder and giving yet more possibilities to criminals for money laundering (FATF, 2008). In addition to the absence of anti-money-laundering obligations, criminals can benefit from the possibility of aggregating large sums by transferring very small amounts of money many times without attracting the application of techniques to monitor suspicious behavior, and then move this money inside the payment system or between different e-payment providers, or from e-payment systems to bank accounts and back.

Thus, e-payment services allow for illegal money transfers either in a way similar to online banking or in the form of transferring cash into online money and further purchase of goods, services, and digital currencies.

Digital currencies

Digital currencies embody a fast-growing area of internet commerce, driven by demand for low-friction e-commerce (Meiklejohn et al., 2013) and micropayments. It is difficult to estimate the number of online payment providers, especially the number that does not conduct due diligence. For example, FATF in 2010 reported that 15 of the jurisdictions responding to the FATF questionnaire indicated that Internet Payment Service providers were operating in their respective jurisdictions without giving the number of such providers; the estimated number of providers in different countries ranged from 1 to 23. With the growth of the digital economy in the last several years, this number could have increased significantly both on the national and international levels. Reliable statistics concerning the number of electronic payment intermediaries, which could show the whole picture on both the international and national levels, are not available. Value exchange systems that operate electronically and make transactions with the currencies that exist only online are not issued by financial institutions and thus are exempted from regulation. These currencies can be exchanged between account holders, or changed into traditional money (FATF, 2015). They are accessible from any part of the world and allow making money transfers instantly, at low cost and with

anonymity (Samani et al., 2013), sometimes leaving virtually no trace. The anonymity of digital currencies and no regulation in this field make this type of payment an attractive option to criminals (Bryans, 2014).

The role of digital currencies in illegal money transfers is prominent and constantly evolving. First, the use of digital currencies for illegal money has been confirmed by several criminal investigations against currency providers, such as E-gold or Liberty Reserve (Samani et al., 2013). Second, it is a well-known fact that digital currencies, like Bitcoin, are used for payments at the online underground markets. What makes the situation even more difficult is that many of those currencies are decentralized and thus hard to control; for example, shutting down Bitcoin requires shutting down the internet because no core node can be taken down. Digital currencies, as a way to transfer money illegally, can be further converted into cash or other means of traditional payments. Illegal markets offer several possibilities for such transfers; there are websites, both in legal and illegal parts of the web, anonymous and non-anonymous, which offer not only to exchange Bitcoins for money via PayPal, Automated Clearing House (ACH), or Western Union, but also to turn Bitcoins into cash sent directly via mail.

According to Europol's predictions, with the further evolvement of cryptocurrencies, it is likely that we will witness the development of more niche currencies, which would be specifically tailored to carry out illicit transfers and will provide greater levels of security and true anonymity. The French anti-money-laundering body, TRACFIN, already mentioned at least two such anonymous and virtually untraceable digital currencies: Zerocoin, which represents an extension to Bitcoin's protocol for greater anonymity, and Darkcoin, which offers fully encrypted transactions and anonymous block transactions (TRACFIN 2014). Further developments in this field also include such applications as Dark Wallet, which makes Bitcoin transactions untraceable and allows for laundering someone's Bitcoins, private cryptocurrencies created solely for the Russian underground market, and others.

Online casinos, e-gaming, and online betting websites

For decades, casinos in the offline world have been considered a sure way to launder ill-gotten money. It is natural, then, those online casinos attracted the attention of law enforcement and regulators as a possible way to use digital technologies for illicit funds transfers. However, despite this conventional wisdom, there have not been many known cases thus far of the use of online casinos for money laundering. A few cases have been detected, however, in the use of e-betting systems. For example, in Australia, an Albanian organized crime syndicate employed an online betting system combined with internet payment services to launder illicit funds obtained from the sale of cannabis. The services were used to receive international transfers and to move money offshore. The online betting service was used in this illegal scheme to store the funds and make them accessible to other network members through sharing account passwords. The value of incoming and outgoing money was counted in the millions of Australian dollars. Therefore, despite the lack of case studies and investigations, such examples prove that online gambling and betting services can be used for illegal transfers, especially when they are combined with online payment systems and digital currencies. As is argued by some researchers, online gambling can allow money to be distanced from the illicit source for the criminal enterprise of any size, both by gambling or by establishing an online casino in an offshore jurisdiction.

E-commerce

Since the internet offers countless possibilities for trading goods, or exchanging money for goods and then selling them further, these activities can certainly be employed as a way for laundering illicit profits. Such schemes as the exchange of illegally obtained money for certain goods and trade of these goods to distance the profit from the source can be a part of the placement or layering stages of illegal money transfers (Villasenor et al., 2011). Another possibility of using the internet for illicit transfers is the establishment of an e-commerce company, be it real or fake, and to offer services or trade goods that are never actually delivered.

A complex landscape of illicit financial flows

As can be seen from the analysis above, the landscape of illicit financial flows on the internet is complex and can be attributed to various online activities and distinct areas of regulation. The convergence of different fields, such as online gambling and digital currencies, e-commerce and e-payments, and telecom services and banking, makes the ecosystem extremely complicated in terms of oversight and control. The internet itself is already a complex and decentralized cross-border network, where the possibility of tracing and prosecuting crimes requires effort and international cooperation. Tackling the problem of illicit financial flows in cyberspace represents a great challenge for regulators and law enforcement agencies because of the complexity and borderless nature of the online environment. The analysis below will focus on the question of how technology can help in tackling the problem of illicit financial flows—both on the internet and in the offline world.

Digital technologies in fighting illicit financial flows

One of the critical issues to consider in the discussion about the nexus of digital technologies and illicit. Financial flows are the question of whether and how technology can be used to address this problem. This question, in turn, should be discussed even in the broader context of the debate on the role of technology in fighting illicit financial flows in the digital era. This debate involves a set of complex issues, which go far beyond the discussion about the choice of particular technologies for investigation or the ways regulators and law

enforcement agencies can use communication information and networks for disrupting illegal activity. The following analysis deals with two main aspects of this discussion: the use of information technologies for empowerment; and the role of digital tools for the prevention, detection, and investigation of criminal activity.

3. Research Methodology

Research Design

The research opted for a descriptive design to establish the relationship between a country introducing digital taxation and reducing illicit financial flows. The research study describes how migration from traditional means of trading to digital avenues has facilitated illicit financial flows in developing countries, which are characterized by weak regulations of the platforms leading to loss of crucial revenue streams.

Target Population

The target population of the study was secondary data from all developing countries. Most of the developing countries are in Africa, Asia, and Eastern Europe.

Sample Size

The target population was too large for the current, hence a random sampling method was used to narrow down the countries to 12. Most of the countries chosen were from sub-Saharan Africa where the vice is prevalent and there is concerted effort to reduce it through the introduction of digital taxation and other technologies.

Data Analysis

Datasets for the current study were found from published data from individual countries and the World Bank from its Global Findex website. The World Bank data in particular was crucial in forecasting the revenue that that developing country should collect with enhanced digital capacity. The year 2017 was used as the base year for the current study with a forecast to developing countries adopting digital technologies helping them achieve higher revenues beyond 2021. Other sources were used to establish the countries that established an increase in revenue by using digital technologies in general. From the data obtained plausible conclusions and recommendations are obtained.

4. Data Presentation, Conclusion, and Recommendations

Results

The tax rate among the sampled countries looked at corporate and individual tax rates in each country. Deriving tax rates from the Economic Freedom report estimates that developing countries would gain from implementing digital taxation. In most of the countries studied the tax rate did not change and the assumption was that 2017 rates applied.

A growing body of literature cites the impact of governments using digital technologies on curbing illicit financial flows. The literature examined in this study suggests that usage of these technologies stimulates tax revenue growth facilitating means of authorities collecting tax from the emerging e-commerce marketplaces and other means favored by fraudsters and money launderers such as online casinos. The results indicate a direct correlation in governments providing an enabling environment for technology access and usage and reducing illicit financial flows while stimulating economic growth. The state bears the responsibility of acquisition and production of advanced technologies and fostering a sustainable legal framework for its tax administration authorities.

Despite the clear correlation between government usage of digital taxation and curbing rampant illicit financial flows, available studies still fail to consider the different types of digital taxation stemming the flow of financial flow of illicit funds. Hence, the current study contributes to the emerging literature on this field by establishing a link between governments emphasizing digital taxation and curbing the flow of illicit funds. The African countries especially struggle with rampant corruption, which is identifiable as the perpetrators move their illicit gains to offshore havens using digital means.

The key findings from the study include:

Accurate measurement of IFFs in the countries remains problematic despite some magnitude of data being available. The data, however, does not capture the full magnitude of public funds that cross-borders illegally impacting negatively on development in the countries.

The most common means used to evade tax in the jurisdictions include mis-invoicing, trade in illicit goods, transfer pricing, corruption, and trafficking of humans and drugs. The forms include grand corruption scandals by the ruling elites since gaining independence from the African countries.

The key facilitators of illicit financial flows include government agencies such as the police, military, and tax governing authorities. MNCs are another important group in facilitating IFFs in developing countries. For example, as stated earlier Flower MNCs in Kenya overstate losses in Kenya while making massive profits in their domicile jurisdictions.

In Sub-Saharan Countries studied like Kenya, she could be losing more than other considered countries because it engaged with several MNCs about infrastructural projects and other public-private partnerships.

The political will to build legitimate and effective states and in that effect, effective tax regimes are lacking fueling tax evasion. The evidence points at weak institutions in the countries and looting and rent extraction.

In Sub-Saharan countries, the impact of IFFs on social, political, and economic development agendas is quite severe. The effect is felt in domestic resources making the countries depend on foreign aid. The poverty situation in the countries is made worse by the flow to foreign havens worsening social development outcomes such as health and education.

Regardless of the overwhelming evidence of the negative impacts of IFFs, there is little impetus that policy actors are aware of and appreciate the magnitude. SDG 16:4 requires that countries reduce the magnitude of IFFs arms flows. Regulation has to improve in the jurisdictions to stem the flow of IFFs. Loopholes exist coupled with inadequate resources making the fight inappropriate. The governments' strategies do not in-calculate MNCs and private sectors in curbing the flow. However, the only bright light is the improved collaboration with international agencies to curb the IFFs.

Conclusion

The current analysis synthesizes published and unpublished literature on the flow of IFFs in Kenya and other Sub-Saharan African countries. The tax reform policies, practices, and policies influence the amount of IFFs in a jurisdiction. The analysis considers what is already a common knowledge on the area from existing evidence while identifying research gaps that need addressing. There are many socioeconomic, development, and institutional policy and legal framework issues involved in dealing with IFFs. The conceptual definition of IFFs is cross-border capital transactions designed to conceal and facilitate illegal activities. The funds are usually illegally earned, transferred, or utilized.

Recommendations

The governments should strengthen tax systems such as using digital taxation systems, surveillance, and collection to curb tax evasion and other capital flights.

There is a need to create awareness of available international instruments and legal obligations in the area.

The fight should include a multi-policy area to design and implement policies and actions in different levels of government.

Reforming government policy interventions to curb IFFs to make them effective.

Engaging offshore financial centers to institute internationally agreed-on counter-measures.

[1.] References

[2.] Bertrand. (2015). Silk Road wasn't even close to the biggest drug market on the internet. http://uk.businessinsidr.com/silk-road-wasnt-even-close-to-the-biggest-drug-market-on-the-

[3.] Blankenburg, S. and Khan, M. (2012). Governance and Illicit Financial Flows.

[4.] Bryans. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution (August 29, 2013). Indiana Law Journal 89 (1). http://ssrn.com/abstract=2317990.

[5.] Council of Europe. (2012). Moneyball report: Criminal money flows on the internet: methods, trends, and multi-stakeholder counter-action. 2013: The use of online gambling for money laundering and the financing of terrorism purposes. Research report.DC: World Bank. Disaggregation. Working Paper for the 2017 World Development Report. Washington,

[6.] Eunomix. (2015). A review of the UNCTAD report on trade mis-invoicing, with a focus on2030 Agenda for Sustainable Development of the Independent Experts.

[7.] 2O12: 18. https://www.sas.com/news/intelligence_quarterly/q312.pdf.

[8.] FATF (Financial Action Task Force). (2008). Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems. http://www.fatf-gafi.org.

[9.] Filipkowski. (2008). Cyber Laundering: An Analysis of Typology and Techniques. International Journal of Criminal Justice Sciences (IJCJS) 3 (1): 27.

[10.] Ghosh. (2012). How to prevent fraud in the Indian telecom industry? Journal of Advanced Analytics 3Q

[11.] https://s3.amazonaws.com/one.org/pdfs/Trillion_Dollar_Scandal_report_EN.pdf.

[12.] internet-2015-6?r=US&IR=T

[13.] Jansky, P. (2013). Updating the Rich Countries' Commitment to Development Index: How They Help Poorer Ones Through Curbing Illicit Financial Flows. Social Indicators Research, 124(1), pp. 1-23. DOI: 10.1007/s11205-014-0779-3

[14.] Malhotra. (2010). A New Dimension of Socio-Economic Offences: E-Money Laundering. July 7. http://ssrn.com/abstract=1505795.

[15.] Massa, Isabella. (2014). Capital flight and the financial system. ODI Working Paper, December 4. http://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9392.pdf.

[16.] Meiklejohn et al. (2013). Fistful of Bitcoins: Characterizing Payments Among Men with No Names.38 (6): 14. https://www.usenix.org/publications/login/december-2013-volume-38-

[17.] National Drug Intelligence Center. (2008). Money Laundering in Digital Currencies. U.S. Department of Justice, Washington, DC.http://www.justice.gov/achive/ndic/pubs28/28675/28675p.pdf.

[18.] number-6.

[19.] OECD. (2014). Illicit Financial Flows from Developing Countries.

[20.] ONE. (2014). Trillion Dollar Scandal.

[21.] Reuter, P. (2016). Illicit Financial Flows and Governance: The Importance of

[22.] Samani et al. (2013). Digital Laundry. An analysis of online currencies, and their use in cybercrime. White Paper, McAfee Labs. http://www.mcafee.com/de/resources/white-papers/wp-digital-laundry.pdf.

[23.] South Africa's gold export Draft final 7 November 2016.

[24.] Thomason. (2009). How has the establishment of the internet changed how offenders launder their dirty money? In Internet Journal of Criminology 2009. http://www.internetjournalofcriminology.com/Thomason_Internet_Money_Laundering_July_09.pdf.

[25.] UN Human Rights Council. (2016). The final study on illicit financial flows, human rights and the

[26.] Villasenor, et al. (2011). Shadowy Figures: Tracking Illicit Financial Transactions in the Murky World of Digital Currencies, Peer-to-Peer Networks, and Mobile Device Payments. The Brookings Institution and the James A. Baker III Institute for Public Policy. http://bakerinstitute.org/media/files/Research/d9048418/ITP-pub-FinancialTransactions-082911.pdf.

[27.] Weaver. (2005). Modern Day Money Laundering: Does the Solution Exist in an Expansive System of Monitoring and Record-Keeping Regulations? Annual Review of Banking & Financial Law 24: 443â465.

[28.] World Bank. (2016). The World Bank Group's response to illicit financial flows: a stocktaking.