Economic Impact of Data Localization in 5 selected African Countries, an empirical study

Mona Farid Badran[1], Associate Professor, Faculty of Economics and Political Science, Cairo University
Rizwan Tufail, Founder, Innovonomics – The Center for Innovation Economics

Abstract:

Nowadays, the important raw material of the global economy seems to be 'Personal Data'. Furthermore, Cross-border data flows lead to a rise in economic efficiency and productivity thereby improving living standards and welfare. However, people are worried about the protection of their data and intrusions into their privacy. In such an environment, faith in data protection laws and regulations, as well as privacy safeguards are the key elements for widespread acceptance and adoption of electronic commerce. Keeping in mind that 107 countries had privacy laws or bills, but only 51 of them were developing countries. The current research paper investigates the impact of laws and regulations that govern the flow of data on the economies of 5 selected African countries namely Egypt, Morocco, South Africa, Kenya and Mauritius using econometric techniques and GTAP database. It reaches the conclusion that fighting the trend of data nationalization is crucial since it hinders the necessary and essential role of the global trade in realizing economic development, especially in the countries under study. Finally, policy recommendations are provided in this respect.

Keywords: data localization; GTAP; trade; cloud computing; economic policy

Jel-classification: L5, L86, L63, L96

[1] Email: mona.badran@feps.edu.eg
Samifarah.mona@gmail.com

1. Introduction

Flow of personal data is essential for the expansion of international trade and co-operation. New challenges like protection of personal data have erupted ever since we have an increase in the intensity of such flows. (Allen and Overy, 2012)

Cross-border data flows lead to a rise in economic efficiency and productivity thereby improving living standards and welfare. For example, trans-border data flow has facilitated interaction with customers in the form business communication in real time, providing business with an ability to decide quickly about various strategies and to further refine designs, processes and services to suit the customer's needs. It has caused disaggregation in the supply chain of businesses in many nations (Samuel Palmisano, 2006).

Most business houses work on international scale, both internally within the global group structures and externally with multiple networks of customers and suppliers. This is not confined to large enterprises; small and medium sized businesses are also adapting to the new facets of technology like 'Cloud Computing' and are now using a large array of products and services to collect, store, use and disclose the data across borders.

Nowadays, the important raw material of the global economy seems to be 'Personal Data'. People are worried about the protection of their data and intrusions into their privacy. In such an environment, faith in data protection and privacy safeguards are the key elements for widespread acceptance and adoption of electronic commerce. The large scale movements, at an international level, of personal data and the rise of electronic commerce have led to economic growth and efficiencies, creating a positive economic trends and outcomes across the globe; these very trends, however, have simultaneously put the privacy, security and well-being of people and businesses at risk in ways that could not have been imagined thirty years ago.

2. Data protection and privacy laws

The enactment of data protection laws in European nations in 1970s was the first time that laws pertaining to data protection and privacy were enforced for trans-border flow of data. Following this, several international organizations rules and regulations, mainly OECD Guidelines, were strongly implemented in 1980s. Convention 108 of the Council of Europe was the first formal instrument that was brought into force at the regional level. The most prominent of all has been the 'EU Data Protection Directive', which contains detailed explanation of the rules that regulate trans-border data flows. All the personal data that is transferred internationally has been provided safety cover by a 'Privacy Framework'(built on the principles of accountability) which was formed by APEC in 2004 and the member

nations welcomed its enactment. Data protection or privacy laws, that regulate trans-border data flows, have been enacted and implemented by more than sixty nations; these laws are mainly based on or draw inspiration from one or more international or regional laws. Almost the entire world has been covered by these laws including regions like North America (Canada); Latin America (Argentina, Columbia, Mexico and Uruguay); the Caribbean (The Bahamas); all European Union member states and the European Economic Area and many other European nations (Albania, Bosnia Herzegovina, Switzerland etc.); Africa (Benin, Burkina Faso, Mauritius, Morocco, South Africa, Tunisia, etc.) the Near and Middle East (The Dubai International Financial Centre and Israel); Eurasia (Armenia); Asia Pacific Region (Australia, Macau, New Zealand, South Korea, etc). Aside from the prevailing laws and legislations, several other factors including voluntary and private-sector systems also influence the movement of data across borders. A collective effort is being made to formulate an International Instrument on data protection and privacy and many regions and nations are presently assessing its need and subsequently implementing it. (Kuner, C., 2011)

Nations with weaker data privacy laws see reduced data import from or exchange with EU countries due to stringent Data Protection laws in EU. This law was initially brought in to resolve data protection issues at various levels, and is not only actively imposed within EU but it is also applicable to third party countries when transferring personal data. Regular assessments are carried out by the EU, and if the data protection in these third-party countries compares unfavourably to the levels of data protection in the EU, these laws would limit the capability of these countries to export services like accounting or advertising that need the personal data to be gathered from EU customers. (Gamberal, C. And Mattoo, A. 2002)

In Russia, a Personal Data Law or OPD Law was implemented on 26 January 2007 and is strictly being enforced since then; some of its features are similar to those of the European Data Protection Directive of 1995. The law includes details that would increase the administrative barrier for companies involved in active business in Russia. A list of requirements have been added including (1) the requirement to allow the personal data to be followed up or forgotten, (2) need of approval for data collection and conveyed to third party, (3) responsibility of the data processor to inform both- the data subject and the authorities in case of data breach, and (4) the need for companies to appoint or designate a responsible person as Data Protection Officer (DPO). A new law 'Clear Data Localization Requirement' was brought into force in July 2014 in Russia. (Mihaylova, I., 2015)

A protection mechanism called Privacy Framework has been devised by the Federal Trade Commission of the United States. All companies that gather and use data must strictly adhere to this

mandatory framework, failing which disciplinary action would be taken against the company (Federal Trade Commission Report 2012).

3. Impacts of data regulations

Data protection laws, with their impact on cross-border data flows, have a major impact on an array of economic sectors (finance, transport, communication, automotive, energy, health, commerce and entertainment) businesses, public service organizations and NGOs (Summer, Rene., 2013). These laws cast a shadow on many sectors and players; data protectionism laws formulated by the government with the intention of reducing cross-border data-flow threats not only effect all companies doing business globally but they also impact pure-play technology companies that are involved in production and innovation, thus impacting the competitiveness of such technology companies (Matthieu Pelissie du Rausas et al., 2011).

In today's global economy scenario, processing data from customers, suppliers and employees outside the borders of the native country of a company is very common, and an established norm of the business. However, these data protection laws severely limit such data flows, and data processing has become almost impossible due to enforcement of this new form of data protectionism. If data processors have to build physical infrastructure in each jurisdictional area of operation because of restrictive and onerous data localization policies, this obviously increases cost, thereby increasing the prices the company has to charge its customers, in effect pulling down the international competitiveness of the company.

Interestingly, although some countries contemplate such roadblocks and restrictions as a way to confine this economic activity within their own territory, reality is that these decisions turn out to be harmful instead of being beneficial. The local positive economic benefits of data localization are often misconstrued or exaggerated. There are a number of factors that drive this. Firstly, the hardware and equipment needed to operate a data centres is expensive, driving up the initial investment required. Secondly, the acute lack of skilled technical staff to operate these data centres in most geographies means the required skills are costly to recruit. Thirdly, the nature of the data centres business is such that while they may create construction job vacancies for short periods, the operation of a data centre require very few highly skilled individuals hired in permanent jobs, particularly when data centres have been tasked to work on cloud-based technologies, which is a result of full scale automation at the centres (Michael Rosenwald, 2011). Thus, the long-term economic benefits that most jurisdictions seek remain elusive.

Moreover, by creating a partition between international providers of these services, and local providers, the protectionist policies unintentionally restrict the creative abilities of the local companies – thus limiting their ability to compete globally. Nations that build artificial 'support systems' to bolster local industry with protectionist policies actually weaken it. Curbing cross-border data flows can restrict access to online data which is not available locally, adversely impacting the country's competitiveness and productivity, while also restricting the ability of citizens to enjoy all the benefits of digital world, including personalized services, e-commerce, entertainment etc. Take the opposite example. When countries allow cross-border data flows, and encourage local businesses to compete globally, these businesses can do wonderful things. Xero, based in New Zealand is known for cloud based accounting software catering to both small and med-sized companies in more than 150 countries (Aaron Schiff, 2015). In spite of the risk of being subjected to severe crack down from the nations that are obstructing the data-flow, this accounting service firm leverages the open data access laws in New Zealand, and provides its customers with uninterrupted back-end computing services to enhance their productivity (Aaron Schiff, 2015).

Forced data localization affects mining, oil and gas companies that are keen to send their data across borders for value-added processing, dampening their ability to drive up the productivity, effectiveness and efficiency of their enterprises. For instance, Shell could have been prevented by localization laws from sending data from a particular location in a country to another, as a result blocking it from using large scale information it accumulates about its wells to form a comprehensive, data-driven view of its activities, including data that can help reduce cost for customers and also minimize detrimental effects on the environment. Thankfully that has not happened. While it may make sense to provide guidelines for dealing with data deemed sensitive to national security, care must be taken to ensure that it doesn't impede corporate innovation. Shell continues to accept voluminous data in its "Smart Fields" applications (Jessica Leber, 2012) and uses that to service its customers better.

Restrictions on the data flow of sensitive information like personal medical data of an individual, as is envisioned in countries like Canada, Australia, Russia and India, may keep companies like Hermes and Alliance Medical from outsourcing data processing services (MRI scan diagnostics), leading to cost escalation in healthcare services, while also increasing the time demands on doctors. These obstacles could also hinder vital medical research, and large scale medical studies on a global scale. Therefore, by obstructing the exchange of medical information, even personally unidentified information, the protectionist policies of a country harm not only its own people but the global community – all people across the world who would benefit from improvisation in the field of medicine (Castro, Daniel. 2015).

The motivation and inspiration for preparing the data protection regulations generally comes from a large variety of sources like the distinct legal traditions and cultures of the nation or region from where it emerged originally. For instance, in some areas (like the EU), legally-binding human rights instruments create the basis of the data protection and privacy laws that are enacted. In other cases, the

motivation may be to create the circumstances to accelerate the development of electronic commerce, e.g. in the APEC region. Nevertheless, widespread enforcement of this kind of regulation can be problematic as it may affect the vital decision-making about data processing made by data controllers. Trans-border transfer of data has increased in parallel with greater participation of individuals on the Internet. This has given individuals greater say and involvement in the management of their personal data but simultaneously trans-border data flows regulations has become more complicated and less transparent, making the entire process less understandable for people. (Kuner, C. 2011) Trans-border data flow seems to be encouraged by four policy objectives namely, (1) preventing circumvention of national data protection and privacy laws; (2) guarding against data processing risks in other countries; (3) addressing difficulties in asserting data protection and privacy rights abroad and (4) enhancing the confidence of consumers and individual. Trans-border data flow is not just risky but it also has associated economic benefits. With the globalisation of the world economy, cross-border data flows have created the engine for innovation as well as improved efficiency and productivity, leading to a consistent rise in economic and social development. The confidence to execute trans-border data flow is critical in safeguarding privacy and building the confidence required to allow personal data to be shared across boundaries; protection of these fundamental rights by the ruling governments goes a long way towards building the required assurance.

Over the past few years, some probing research has been conducted to understand the effects of trans-border data flow regulations more fully (Kuner, C. 2011). This body of research shows that there is a direct cost from data localization mandates in the form of negative impact on the GDP. While the impact is quite clear in the case of sector-specific data localization, there is an even more pronounced impact if all sectors of the economy in the nation are impacted by data localization requirements. For instance, it was reported in 2013 that if cross-border data flow were interrupted in the European Union, the adverse effect on its GDP would be between -0.8 to -1.3 percent and production exports to United States of America by European Union may fall by about 11 percent (Bauer Matthias et al. 2013). On the contrary, according to 2013 estimations, reducing the obstructions to cross-border data flow would enhance GDP in United States of America by 0.1 to 0.3 percent (United States International Trade Commission, 2013). Hence enforcing limitations on cross-border data flow has negative impact on the global competitiveness of the nations implementing these regulations and also the others in the global economy (Stephen Ezell et al. 2013).

Since data regulations restrict the ability of businesses and individuals from making full use of data, and in effect increase the cost of services that require data, it stands to reason that prices of any goods or services that use data in their production would also increase. In many sectors of the economy, data regulation leads to productivity losses at domestic level. This gives rise to another trade obstruction against data processing and internet services, or any other service that depends on the usage of data for

delivery. As the competitive landscape of the economy changes, investment will be affected. The effectiveness of R & D is affected to the extent that product development depends on customer and market data to compete in the market place. (Bauer, Matthias, et al., 2014)

Domestic and International organizations may have to bear heavy cost for cross-border data rules and the new rules that may be introduced (Berry and Reisman, 2012). Very little is known about the process through which rules on data flow affect the functioning of the industries. There is no formal evaluation to study how data regulations may impact the performance of domestic industries. From a general perspective, service businesses are now influenced by a new costly feature, which is a direct result of the regulation of data flow; it only impacts how the (personal) data is used and further processed by the companies during the interaction between customers and producers or only a set of producers. Instances like swiping a credit card (while making a payment) are some of the occasions when a customer's (personal) data gets transferred and is used by the companies; another example is while using social media websites for healthcare services. Cross-border transfer of data both domestic and international terms particularly increases when the customer and manufacturer are located geographically far apart from each other. Trading of data among different groups or countries is controlled by Data Flow Regulations. (E. van der Marel et al, 2015)

To cite an example, consider a customer in his home country making a payment by his credit card at his bank affiliate. During the process of the transaction, data from the card is copied onto a server which may be located far away geographically. The stored data is then used for processing at the headquarter of the bank's affiliate that may be situated in some other country. In this case, regulation of the market helps protect consumers in the market from negative spill-over outcomes or externalities that could result from unprofessional or unscrupulous actions by any of the players, in pursuit of higher profit margins. Privacy protection is of paramount importance in this sector; apart from this there is very little that can cause market failure in this sector of data services as these services have always been positively accepted by consumers. The main issue here is the potential for compromising the protection system that are in place to safeguard the personal data of the consumers which is used and processed by the third parties and later stored on their servers. Customers are unaware of their data transfer from their credit cards to the servers of the intermediate service providers, during the transaction and also about its processing and storage at a later stage. The challenge for policymakers is to devise necessary rules and regulations which are connected to a particular social objective (or negative externality) and implement these rules and regulations at the lowest possible cost in terms of economic welfare, to prevent them from putting unwanted burden of cost on the companies. This is viewed as the main challenge for experts in policies, which is quite similar to other sectors (Saez et al., 2014).

New rules and regulations can have harmful economic impacts on the cross-border movement of personal data of the customers, which is meant to be used by the producers, as examined by Bauer et al.

(2013). This is caused due to the fallout of data services regulations that restrain transaction between domestic and multinational operators; this then results in limiting the choice of competent and acceptable providers of data processing activities. (Miroudot et al. 2009).

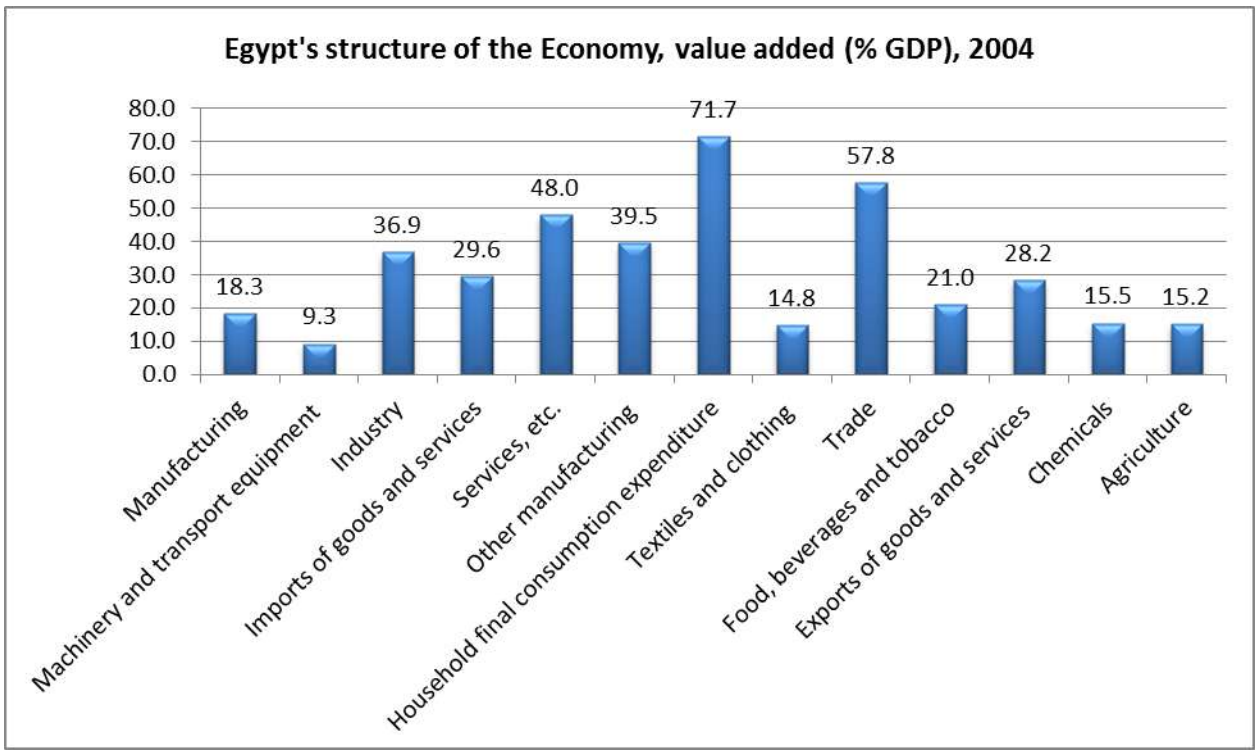
Data is largely used by the services sector. Regulatory limitations in the data transfer negatively impacts downstream performance in various sectors of the economy in which data processing is a significant component of production activities, e.g. value-added business services or financial services. Apart from other factors, regulations are also often necessary in managing competitive situations that affect services after the completion of a process of deregulation or liberalization. However, not all the rules and regulation in general, or that of data in particular, are useful in removing these negative externalities. Storing all the consumer data inside a geographical region may heighten negative externalities by risking that data might be attached broken into, at the orders of a government, or because of a lack of world-class security systems. This development is known as 'Honey Pot Syndrome' in the industry. It leads to incurring of additional cost to the local users of the data; it leads to situations in which central storage for the data is achieved, without properly resolving the market failure issue. (E. van der Marel et al et al. 2015)

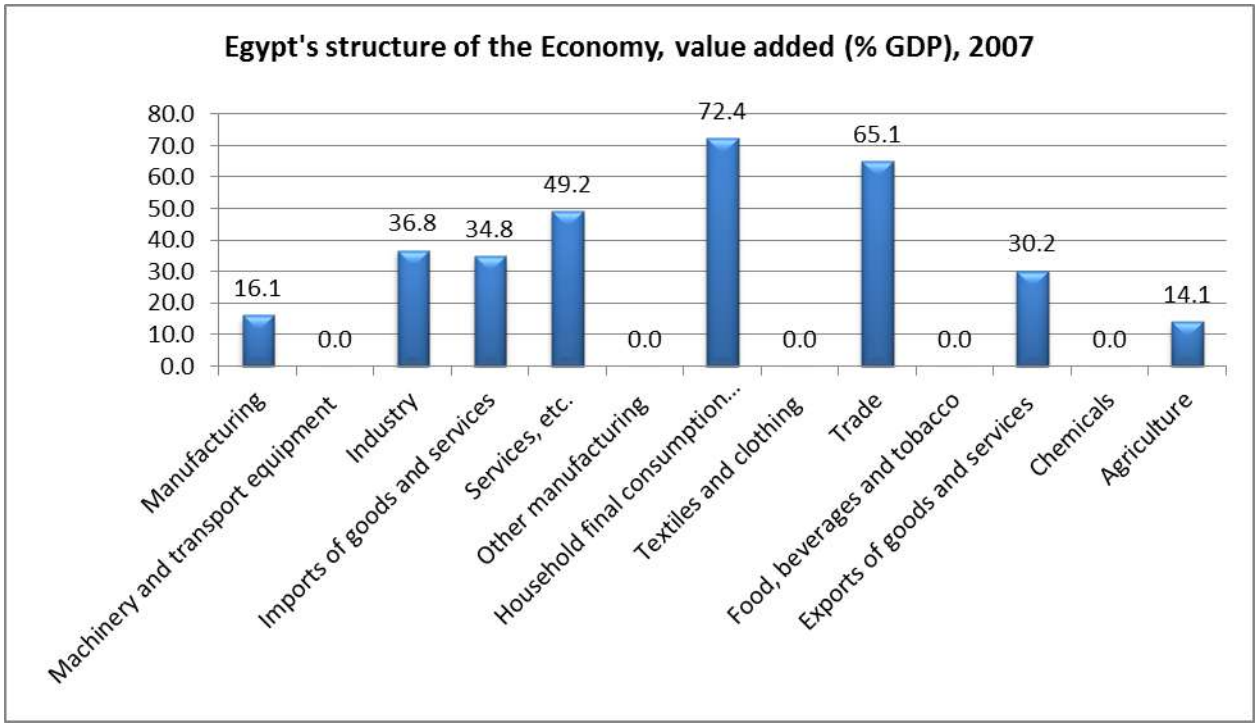
Data regulation is an urgent need of each nation to protect its personal data. But at the same time, these regulations create hindrances for the smooth functioning of an economy. In the modern world, economies are interconnected and data of one country is either used by the other, or is built upon by companies operating in another country. There has been very little research in this direction, particularly in understanding the impacts of data regulations for emerging markets. This study will play a significant role by contributing to the existing literature.

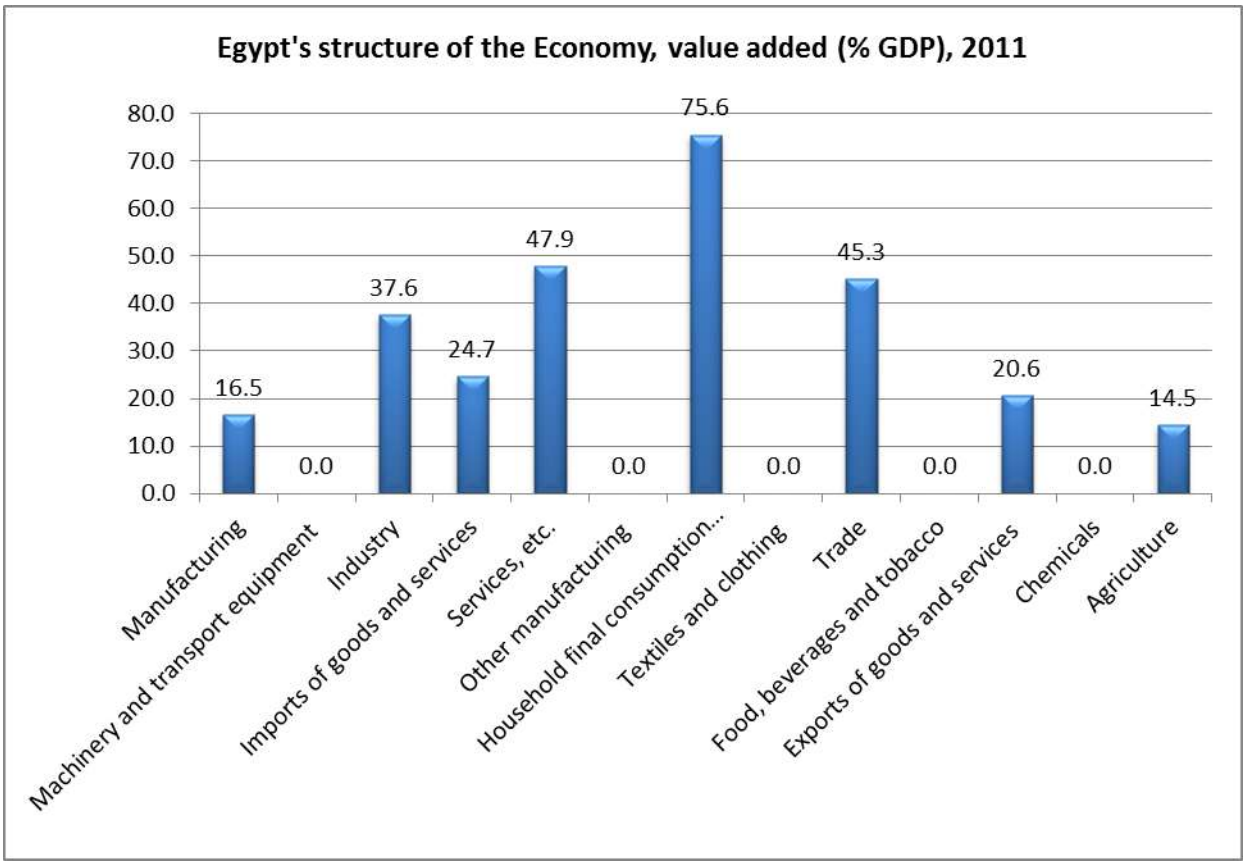
4. Economic structure of selected African Countries

In Egypt, during the three years under study 2004, 2007 and 2011, the composition of the economy didn't change largely from a dominating services sector with the share of around 47 percent of the GDP, followed by the industry sector with about 37 percent share of the GDP and finally the rest is the share of agriculture in the GDP by about 15 percent.

Economy structure of Egypt:

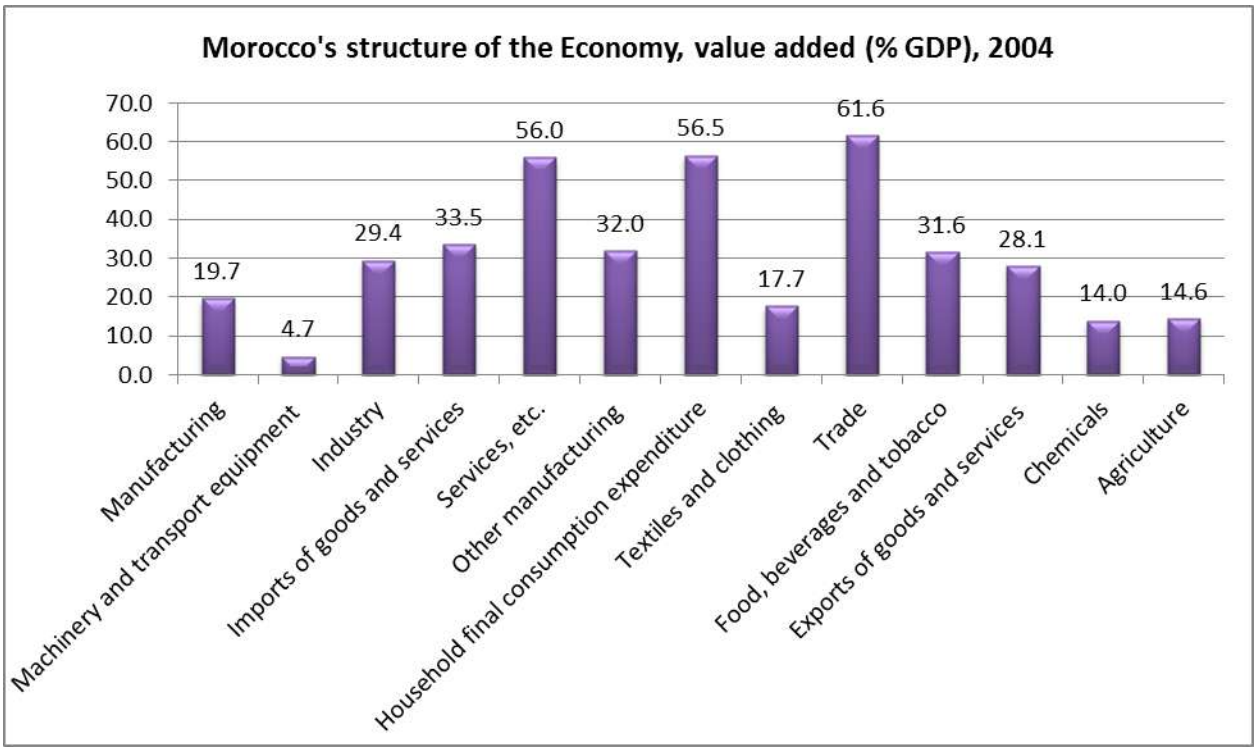

Egypt's structure of the Economy, value added (% GDP), 2004
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
18.3
9.3
36.9
29.6
48.0
39.5
71.7
14.8
57.8
21.0
28.2
15.5
15.2
Manufacturing
Machinery and transport equipment
Industry
Imports of goods and services
Services, etc.
Other manufacturing
Household final consumption expenditure
Textiles and clothing
Trade
Food, beverages and tobacco
Exports of goods and services
Chemicals
Agriculture

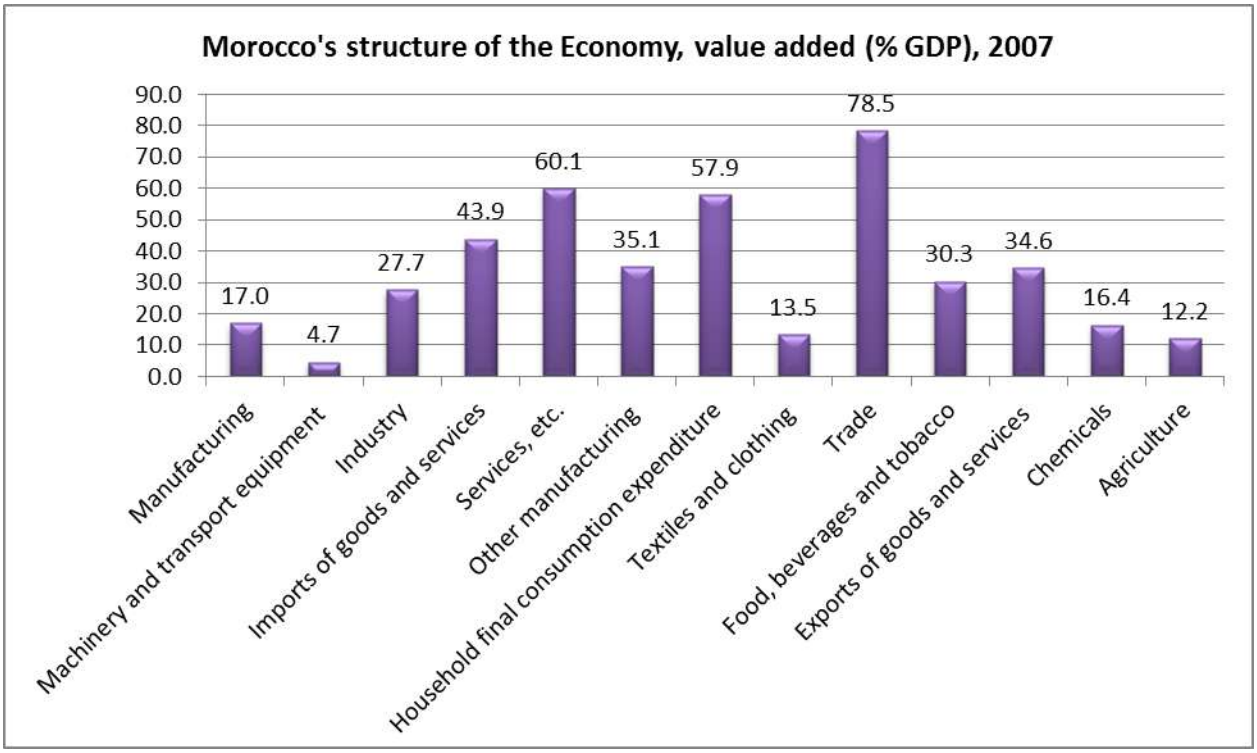

Egypt's structure of the Economy, value added (% GDP), 2007
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
16.1
0.0
36.8
34.8
49.2
0.0
72.4
0.0
65.1
0.0
30.2
0.0
14.1
Manufacturing
Machinery and transport equipment
Industry
Imports of goods and services
Services, etc.
Other manufacturing
Household final consumption...
Textiles and clothing
Trade
Food, beverages and tobacco
Exports of goods and services
Chemicals
Agriculture

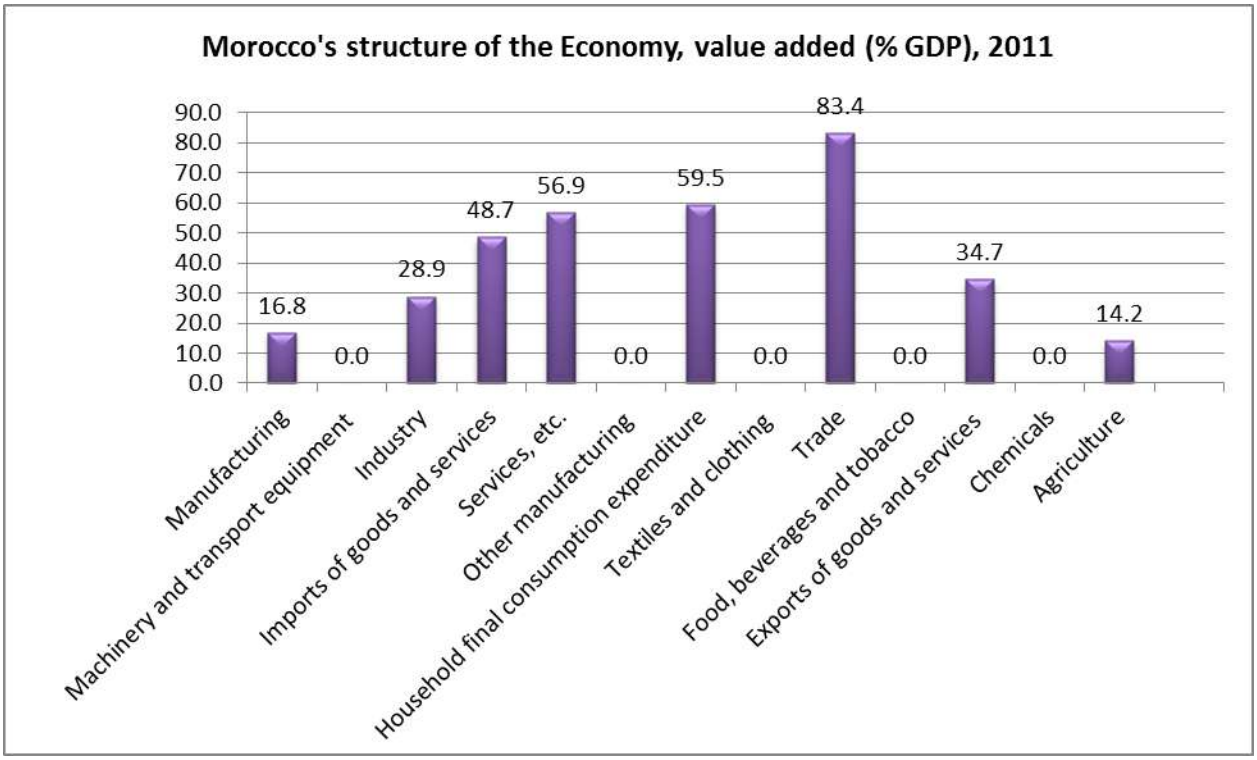


Morocco, has a similar composition of the economy as Egypt but with a slightly larger services sector around 57 percent in 2011. And an industry sector that amounts to the 30 percent of GDP and finally agriculture sector that dropped in 2007to reach 12.2 percent of GDP and increased in 2011 to the level of 14 percent share of GDP.

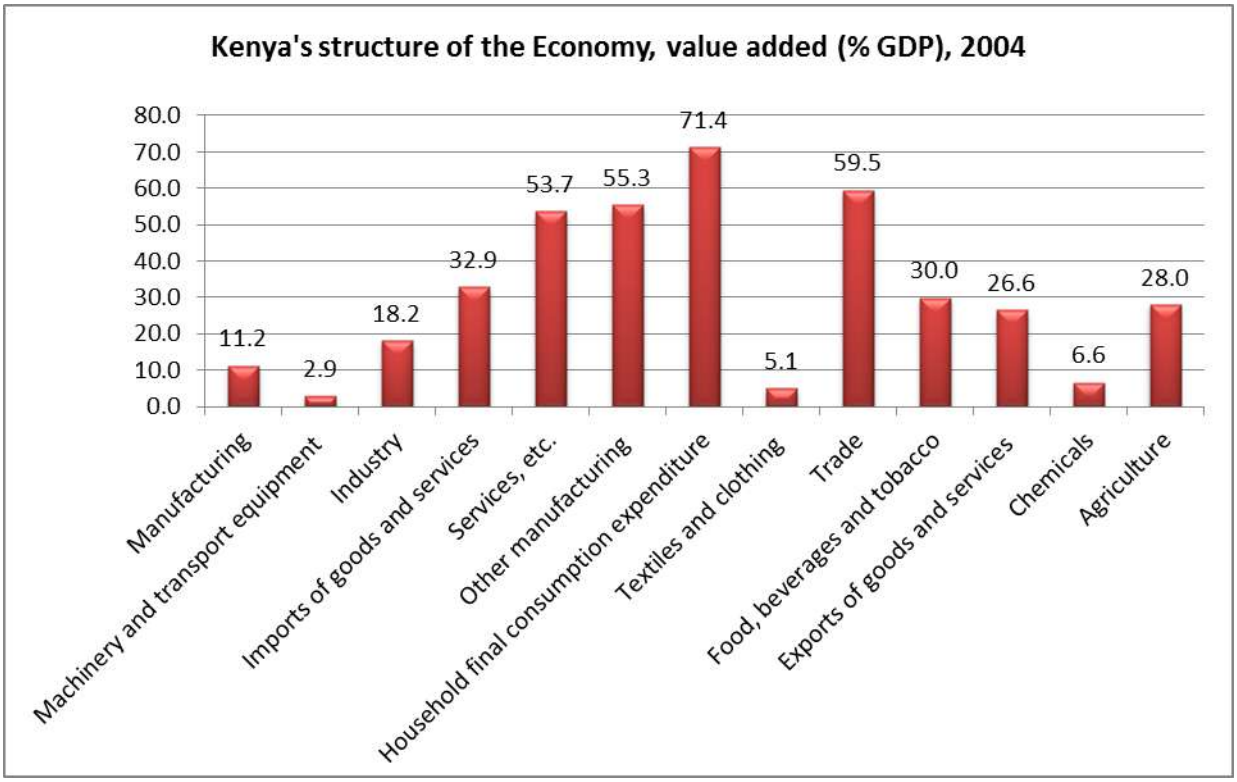
1. **Economy structure of Morocco:**

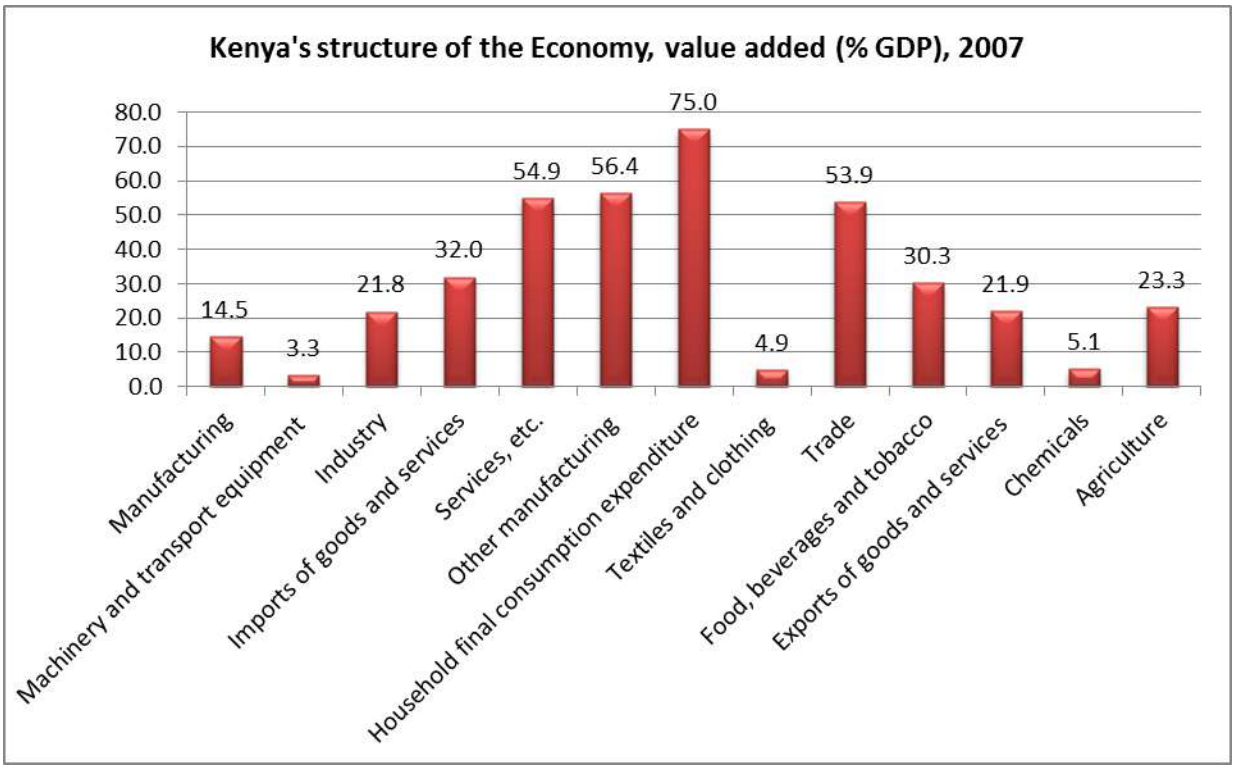

Morocco's structure of the Economy, value added (% GDP), 2004
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
19.7
4.7
29.4
33.5
56.0
32.0
56.5
17.7
61.6
31.6
28.1
14.0
14.6
Manufacturing
Machinery and transport equipment
Industry
Imports of goods and services
Services, etc.
Other manufacturing
Household final consumption expenditure
Textiles and clothing
Trade
Food, beverages and tobacco
Exports of goods and services
Chemicals
Agriculture

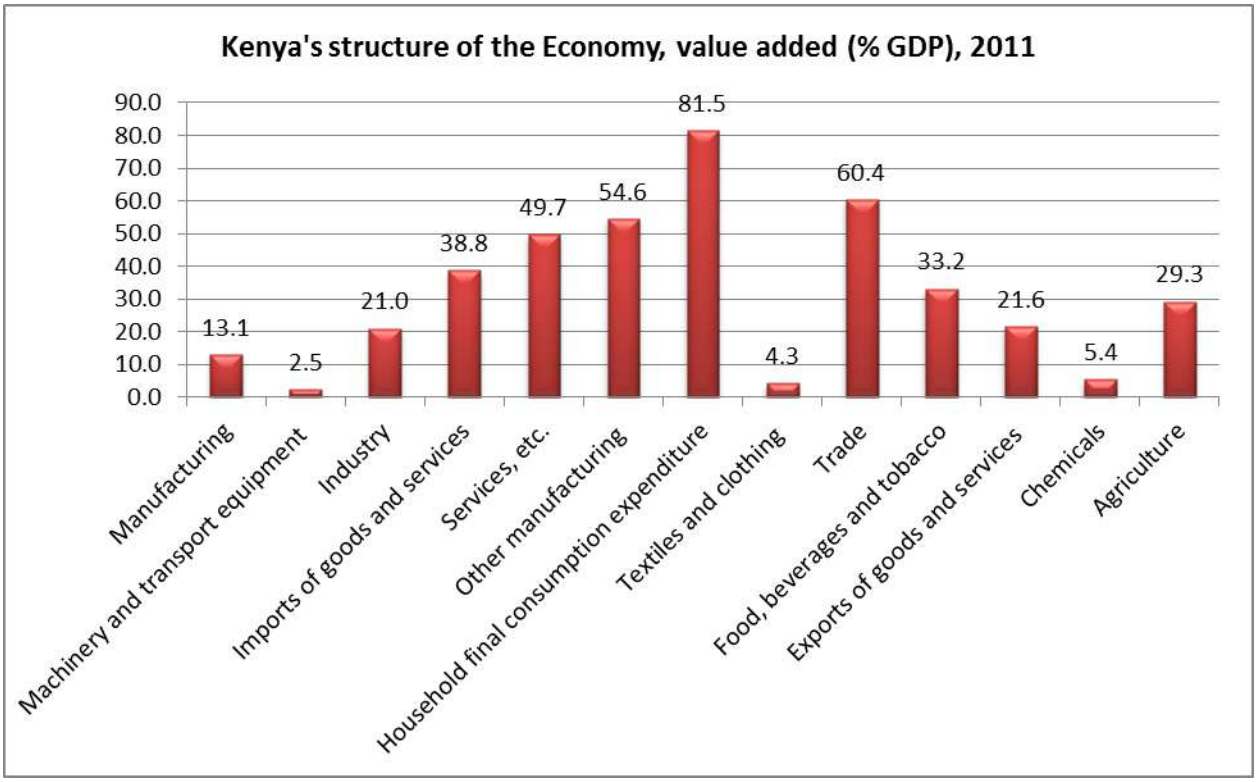

Morocco's structure of the Economy, value added (% GDP), 2007
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
17.0
4.7
27.7
43.9
60.1
35.1
57.9
13.5
78.5
30.3
34.6
16.4
12.2
Manufacturing
Machinery and transport equipment
Industry
Imports of goods and services
Services, etc.
Other manufacturing
Household final consumption expenditure
Textiles and clothing
Trade
Food, beverages and tobacco
Exports of goods and services
Chemicals
Agriculture


Morocco's structure of the Economy, value added (% GDP), 2011
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
16.8
0.0
28.9
48.7
56.9
0.0
59.5
0.0
83.4
0.0
34.7
0.0
14.2
Manufacturing
Machinery and transport equipment
Industry
Imports of goods and services
Services, etc.
Other manufacturing
Household final consumption expenditure
Textiles and clothing
Trade
Food, beverages and tobacco
Exports of goods and services
Chemicals
Agriculture

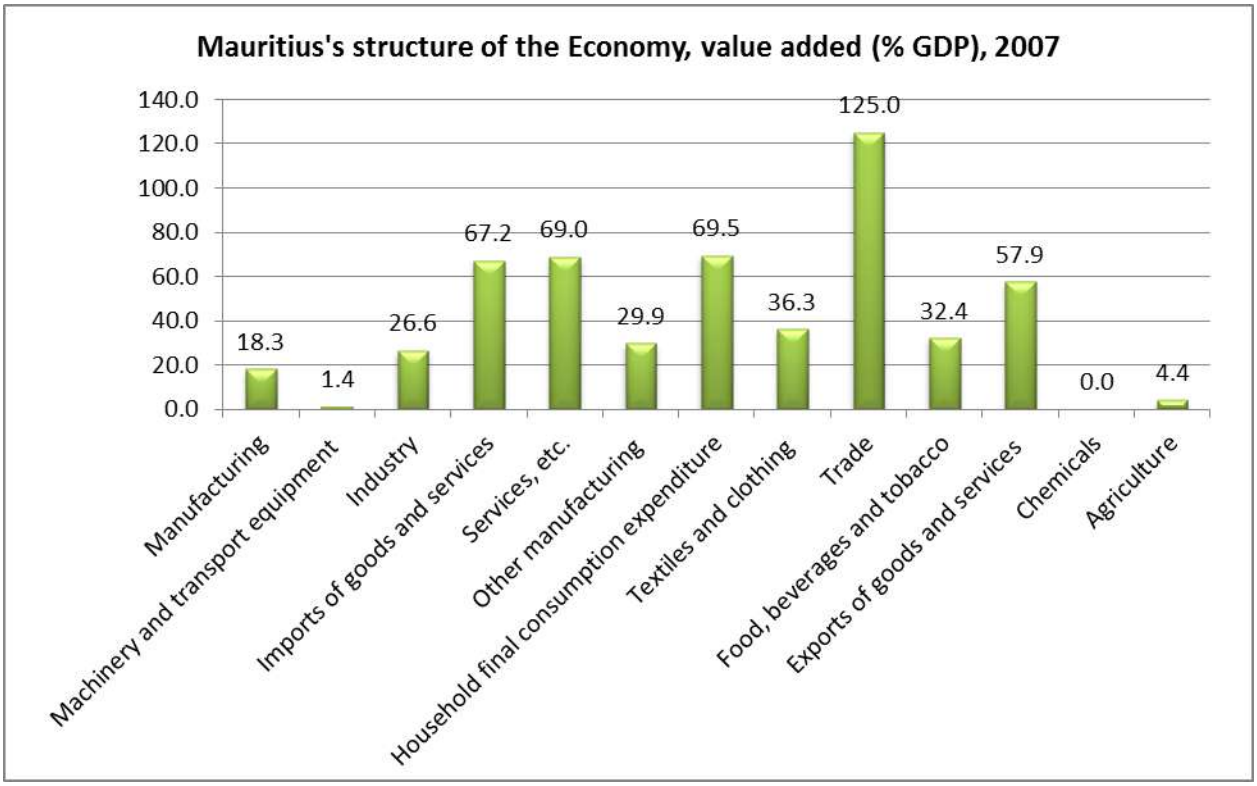
Kenya had a higher share of its services sector of the GDP that amounted to 54 percent in 2004, however, this share was on a declining trend and reached 50 percent as the share of the services sector in GDP in 2011. Furthermore the industry sector share of the GDP experienced an increase from 2004 to 2011 to reach the level of 21 percent of GDP in 2011. Finally the agricultural sector witnessed a sharp decline between 2004 to 2011 from 28 percent to 21 percent respectively.

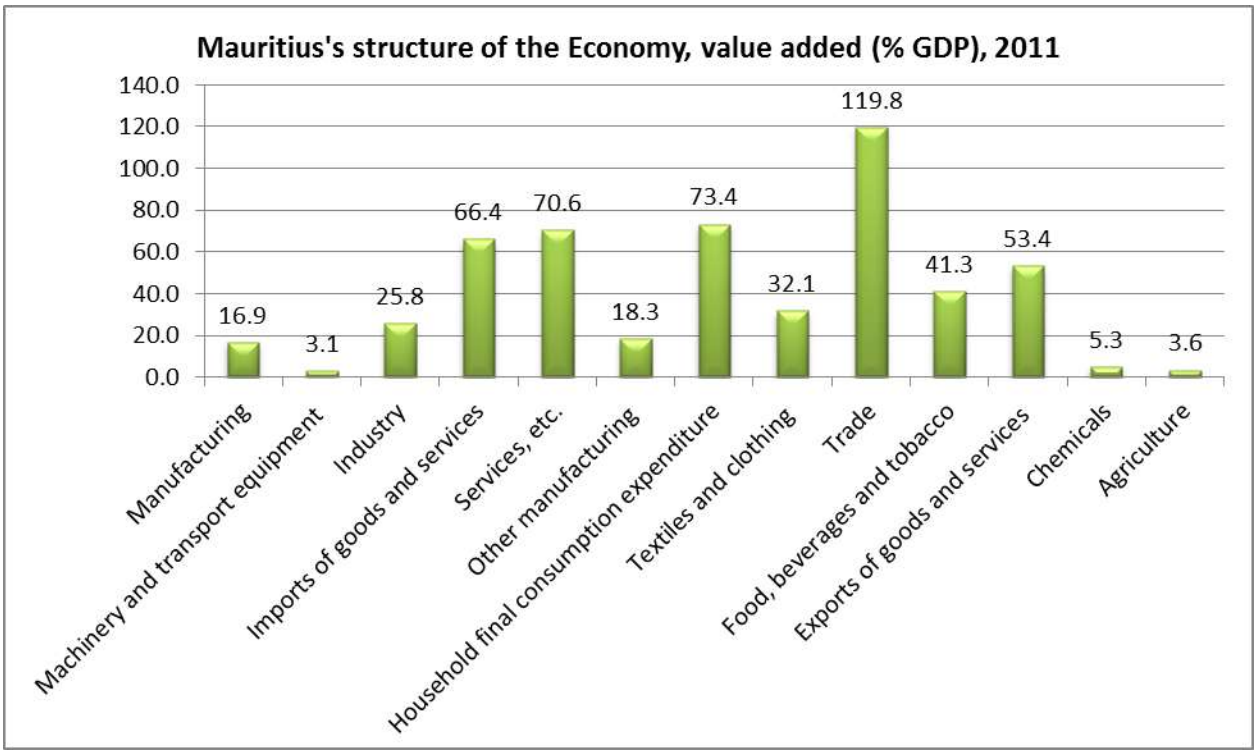



Kenya's structure of the Economy, value added (% GDP), 2007
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
14.5
3.3
21.8
32.0
54.9
56.4
75.0
4.9
53.9
30.3
21.9
5.1
23.3
Manufacturing
Machinery and transport equipment
Industry
Imports of goods and services
Services, etc.
Other manufacturing
Household final consumption expenditure
Textiles and clothing
Trade
Food, beverages and tobacco
Exports of goods and services
Chemicals
Agriculture

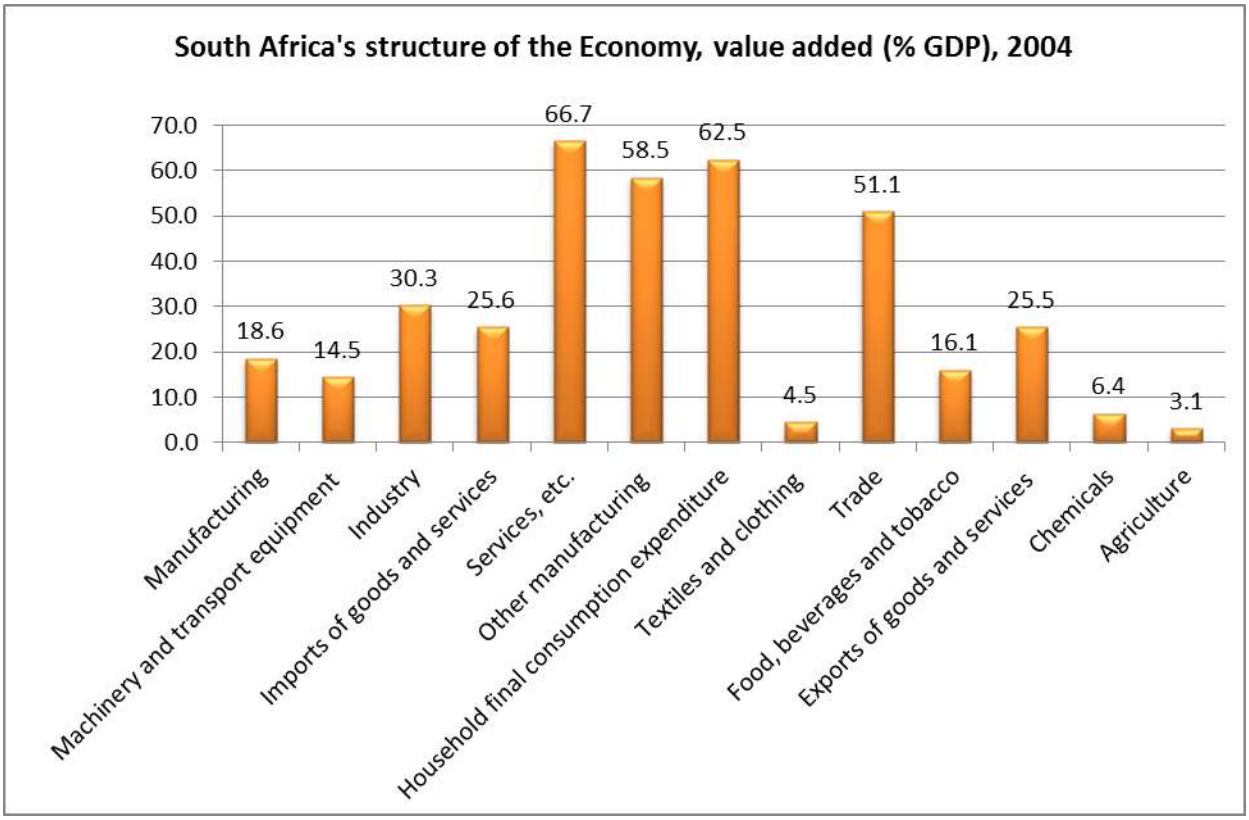

Kenya's structure of the Economy, value added (% GDP), 2011
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
13.1
2.5
21.0
38.8
49.7
54.6
81.5
4.3
60.4
33.2
21.6
5.4
29.3
Manufacturing
Machinery and transport equipment
Industry
Imports of goods and services
Services, etc.
Other manufacturing
Household final consumption expenditure
Textiles and clothing
Trade
Food, beverages and tobacco
Exports of goods and services
Chemicals
Agriculture

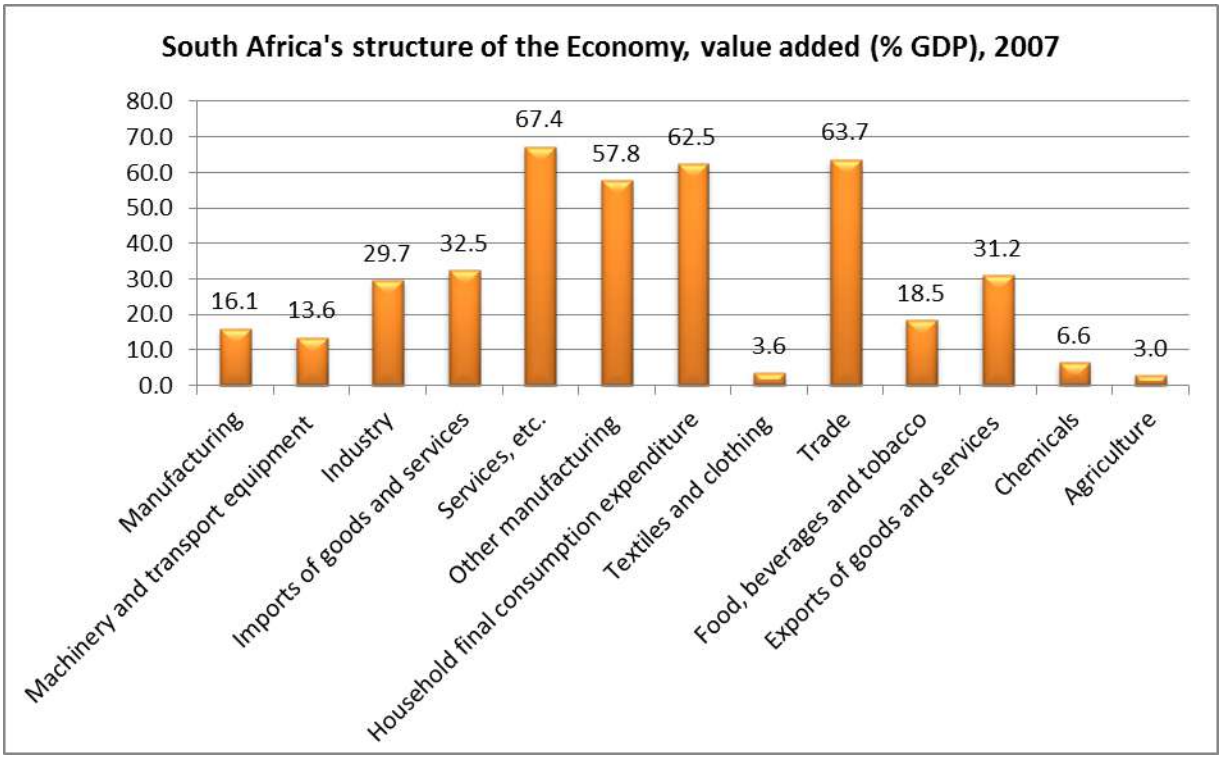
Mauritius stands out with highest share of services sector in GDP to reach the level of 71% in 2011 among the 5 countries under study. The industry sector on the other hand reported a declining trend as a percent of GDP from 29 percent in 2004 to 26 percent in 2011. Then the share of agriculture sector in GDP also witnessed a decline from 6.4 percent in 2004 to 3.6 percent in 20011.

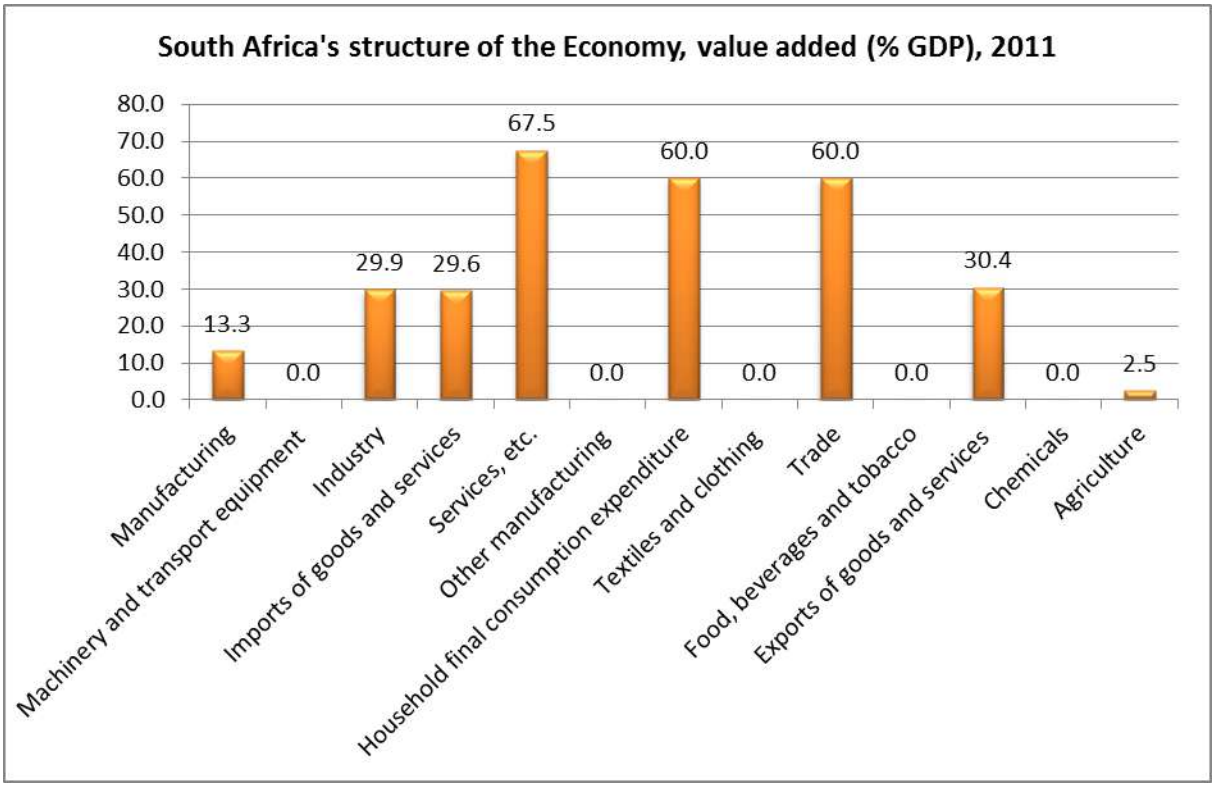




South Africa has a similar structure of the economy as Mauritius in terms of the breakdown of the economy into a dominating services sector, declining share of industry in GDP that amounts to 30 percent of GDP and finally very week agriculture sector with about 2.5 percent share in GDP.


South Africa's structure of the Economy, value added (% GDP), 2004
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
18.6
14.5
30.3
25.6
66.7
58.5
62.5
4.5
51.1
16.1
25.5
6.4
3.1
Manufacturing
Machinery and transport equipment
Industry
Imports of goods and services
Services, etc.
Other manufacturing
Household final consumption expenditure
Textiles and clothing
Trade
Food, beverages and tobacco
Exports of goods and services
Chemicals
Agriculture


South Africa's structure of the Economy, value added (% GDP), 2007
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
16.1
13.6
29.7
32.5
67.4
57.8
62.5
3.6
63.7
18.5
31.2
6.6
3.0
Manufacturing
Machinery and transport equipment
Industry
Imports of goods and services
Services, etc.
Other manufacturing
Household final consumption expenditure
Textiles and clothing
Trade
Food, beverages and tobacco
Exports of goods and services
Chemicals
Agriculture



2. Laws & Regulations governing data in selected African Countries:

2.1 Egypt:

When the government in Egypt blocked all Internet services to the country, at the height of anti-government protests in early 2011, it came as a shock to many. Although there have been instances worldwide of autocratic regimes limiting internet and radio access, this seemed the first time that a country with a modernizing economy blocked access to the Internet, resulting in a 90 percent drop in Internet traffic to and from Egypt.[23] This action, aside from their political and social outcomes, resulted in short-term and long-term impacts on the economy, with immediate loss of nearly $90m to the telecommunication sector, in terms of revenues lost from services it could not deliver[4], and a much longer-term impact on the economy, particularly through the impact of communication services on sectors like tourism, manufacturing and others. Beyond that, this action by the government also

[2] http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?_r=0
3 http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/HowEgypt-shut-down-the-internet.html
[4] http://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm

undermined the confidence of international investors in terms of business continuity, no doubt casting a longer term shadow on the economy.

Much has changed across the world, and in Egypt, since then, both politically as well as technologically. The growing adoption of cloud computing services for personal, government and business across the world, has made telecommunication services an even more integral and foundational part of life. The Snowden episode has brought the issues of privacy and national security, to the front, and countries across the world are assessing how to balance these and other conflicting goals. Like many other countries across the world, the government of Egypt is keeping a close eye on these developments.

It is interesting to observe that on paper, at least, there are no laws in Egypt that specifically govern life in a digital world awash with data. As an example, Egyptian law does not have any specific provisions which regulate online privacy, and it does not have any specific provisions which regulate electronic marketing, and the conduct of such marketing services.

There is no general data protection law in Egypt, and there is no national authority responsible for data protection in Egypt, even if certain types of data and information are protected by specific laws and the constitution. Article 57 of the Egyptian Constitution promulgated in January 2014 provides for the protection of privacy and secrecy of, inter alia, mails, phone conversations and other methods of communication. It was mandated that these could not be monitored, inspected or confiscated without a prior court order and even then, for a limited period of time as regulated by the law. he Egyptian Constitution has not defined data protection. However, it referred to the legislative authority to regulate the communication of data in a manner that does not encroach upon the privacy of citizens, their rights and National Security.

However, there has been little progress in translating these articles in the constitution into laws that would operationalize these intentions. Media reports [5]disclosed discussions in Parliament about a new Cyber Crime Bill, but there was widespread concern that its focus seems to be more on regulating speech and expression, rather than protecting individual rights; the creation of a High Council for Cyber Security[6], before the legislative framework that would govern its operations was highlighted as a risk by many. Additionally, a leaked tender document from the Ministry of Interior revealed plans to conduct mass surveillance of social media by systematically monitoring Facebook, Twitter and YouTube and possibly mobile phone applications such as WhatsApp, Viber and Instagram; the move was characterized

[5] http://www.al-monitor.com/pulse/originals/2016/06/egypt-enacts-cyber-crime-law-preserve-national-security.html
[6] http://www.al-monitor.com/pulse/en/originals/2015/01/egypt-cyber-security-council-privacy.html

by civil society organizations as an attack on internet privacy and freedom of expression[7], and highlighted once again the urgent need for legislation – and enforcement - that protects individuals freedoms and privacy online, not only from criminals but also from their own administration.

At the current time, Egypt does not have a law governing protection, and the use of, personal data. There are indeed piecemeal provisions related to data protection in different laws and regulations in Egypt. As an example, constitutional principles concerning individuals' right to privacy under the Egyptian Constitution as well as general principles on compensation for unlawful acts under the Egyptian Civil Code govern the collection, use and processing of personal data. Additionally, the Egyptian Penal Code no. 58/1937 imposes criminal punishment for unlawful collection of images or recordings for individuals in private places. Other laws that provide for protection and confidentiality on certain data and within define contexts, include

- Egyptian Labour Law no. 12/2003 (confidentiality of the employee's file information including punishment and assessment)
- Egyptian Banking Law no. 88/2003 (confidentiality of client and account information).
- Egyptian Civil Status Law no. 143/1994 provides for the confidentiality of citizens' civil status data.
- The Executive Regulations of Mortgage Finance Law no. 148/2001 issued by virtue of Cabinet Decree no. 1/2001 as amended by Prime Minister Decree no. 465/2005 has clauses that ensure confidentiality of the data of the clients of mortgage finance companies.
- The Egyptian Telecommunications Law no. 10/2003 safeguards the privacy of telecommunications and imposes penalties which account to imprisonment in some cases on the unauthorized violation of such privacy.
- The Mentally Disordered Care Law no. 71/2009 has clauses that ensure confidentiality of the patient's data.

One of the problems of not having a predominant data protection law is that there is no definition of personal data, private life or sensitive personal data under Egyptian law, the Constitutional Declaration or the New Constitution. Egyptian law does indeed provide examples, on a case-by-case basis, of the personal data that are protected under that particular law. Article 77 of the Labour Law, for example, provides that the employees' files that must be kept by the employer (as mentioned below) includes the employee's personal data such as his name, job, professional skills when he joined the workplace, domicile, marital status, salary, starting date of his work, the holiday leave he takes, punishments imposed on him and the reports of his superiors on his work. There is however, no universal

[7] https://www.amnesty.org/en/latest/news/2014/06/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression/

definition of sensitive personal data under Egyptian law. This lack of an agreed-upon definition makes it difficult to legislate to protect it, and, with relevance to online data flows, makes it difficult to argue for different classification, and treatment or protection, of different type of data.

Similarly, there is lack of clarity around the appropriate use of the data, and the penalties for an infringement. According to the Egyptian Civil Code, the collection, use or processing of personal data is prohibited in case it violates the individual right to privacy and provided that such collection, use or processing constitutes a fault pursuant to the Egyptian Civil Code. A fault is defined by the judiciary, and is based on an act or omission that violates an obligation imposed by the law or runs contrary to assumed caution and care of the average man.

Finally, there is ambiguity around how the data can be collected. Currently, only data which is considered relevant to the subject's private life requires his/her consent for collection. Only a competent court will determine whether specific data is considered pertinent to the private life of the subject or not and whether the collection or processing of such data violates an obligation imposed by the law or is evidence of a lack of caution and care that can be assumed of the average man. This means that ex-ante, it is difficult for a data processor to know what level of care to taken when collecting which element of personal data.

Note that the collection of data about the employee is required by law (Article 77 of the Egyptian Labour Law) which stipulates that that each employer must keep a file for each employee which includes their personal data. Only certain persons are authorised by the law to have access to such data.

The same general principles applicable to data collection and processing indicated above apply to the transfer of data; the data controller may not transfer data pertinent to the private life of the data subject except after obtaining the consent of the data subject, unless otherwise permitted by the law. Once again, the implication for a data processor is clear. It is difficult, if not impossible, to know ex-ante what data related to an individual can be moved offshore for processing, without exposing the firm to the vagaries of the interpretation of 'private life' and 'private data' by a court at some later date. As is clear, this does much to reduce business confidence, and introduces unnecessary ambiguity and concerns.

2.2 Kenya:

In Kenya, like in many other African countries, legislation and regulations covering the digital sphere have been helped if not driven by economic interests. A Data Protection Bill was drafted in 2012, circulated widely for feedback, and a subsequent draft forwarded to the Attorney General for publication. Over the past years, there have been numerous reports that the Bill is ready to be tabled to Parliament,

but that has not yet happened. As of the writing of this report, the Data Protection Bill 2013 still awaits presentation in front of parliament, debate and then adoption.

As hinted above, the Data Protection Bill is being discussed as part of wider strategy by the Kenyan government called the 'Connected Kenya Master Plan (2012-2017)', which 'envisions the country as a globally competitive and respected knowledge-based economy [with] strengthen[ed] ICT business development.' The bill has been prepared alongside legislation on access to information which, if passed, would give effect to Article 35 of the Kenyan Constitution which provides for citizens' right to access to information held by the country.'

The Data Protection Bill recognises that 'data protection in relation to personal information is a corollary to the expectation of privacy, a human right that is in keeping with best international practices', reads the Bill's Memorandum. 'The Bill is borne out of the realisation that data protection is crucial for the promotion of e-transactions in the global digital economy where a lot of information is processed automatically.'[8]

In the absence of the data protection bill, principles of privacy are protected by other more general, but broadly applicable legal instruments, including (1) Constitution (Article 31 specifically protects the right to privacy), (2) the 2009 Kenya Information and Communications Act which, under (a) its Article 31 penalises the unlawful interception of communications by service providers), (b) Article 83 which criminalizes wilful interception and provides guidelines for retention of data, and (c) Article 93 which provides guidance on data disclosure, and (4) the Kenya Information And Communications (Consumer Protection) Regulations, 2010, which makes it a criminal offense to monitor communication. However, these protections, particularly against surveillance, have eroded somewhat through recent developments, including (1) 2012 National Intelligence Service (NIS) Act, article 36 of which allows the rights to privacy set out in Article 31 of the Constitution, to be "limited in respect of a person suspected to have committed an offence to the extent that subject to section 42, the privacy of a person's communications may be investigated, monitored or otherwise interfered with", and also by (2) The Prevention of Terrorism Act 2012 which grants extensive powers to state authorities to limit fundamental freedoms and encroach on the right to privacy through surveillance. In light of the challenges highlighted above, the data Protection Bill when passed, would enshrine data protection further, and define clearer boundaries.

[8] http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2306

Once law, the Data Protection Bill will give effect to Article 31(c) of the Constitution, which outlines the right of every person not to have "information relating to their family or private affairs unnecessarily required or revealed" and Article 31(d), the right not to have " the privacy of their communications infringed". It will also regulate the collection, retrieval, processing, storing, use and disclosure of personal data. Yet the proposed legislation does not explicitly address the protection of data stored in the "cloud" (synchronised storage centres for digital data). Nevertheless, the enactment of the Data Protection Bill is crucial in that it will provide a clear legal framework on how personal information — from medical records, identification, banking information, educational records — being held by private and public institutions is stored, retrieved and disclosed to ensure that constitutional safeguards are clear, and subsequently enforced to protect the rights of individuals.

The proposed Bill will also provide clarity around exceptions. As an example, 31 of the Kenya Information and Communication Act clearly states that licensed telecommunication operators are legally prohibited from implementing technical requirements necessary to enable lawful interception, and section 15(1) of the Kenya Information and Communications (Consumer Protection) Regulations 2010, states that a licensee "shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data".

However, the recently adopted Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations 2014 permit access to private or confidential information on consumers without a court order.

One concern is contradicting legislations and guidelines that could come in, due to the prolonged delay in passing the Data Protection Bill. As an example, in December 2015 Kenya's Communications Authority invited the public to comment on the draft Kenya Information and Communications Regulations 2016. Clause 10 (1) of the Cybersecurity Regulations introduced requirements on data localisation which, irrespective of their merits and demerits, could be more stringent, or at odds with the Data Protection Bill once it is finally approved. [9]

2.3. Mauritius:

Mauritius has a strong legal framework and executive processes in place to ensure protection of personal data. It not only has a long history of involvement in these issues, but also is only the second

[9] https://www.article19.org/data/files/medialibrary/38413/Kenya-Cyber-Security-and-Electronic-Transactions-Legal-Analysis-21-April-2016.pdf

non-European state, after Uruguay, to ratify the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, also known as "Convention 108"[10].

Convention 108 is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data, and which at the same time seeks to regulate the trans-frontier flow of personal data. In addition to providing guarantees with reference to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected. The Convention also imposes some restrictions on trans-border flows of personal data to States where legal regulation does not provide equivalent protection. Mauritius has already ratified the treaty, and it will enter into force on 1 October 2016.[11]. Being a signatory to the convention not only assures its own citizens of the highest standards of protection available to their data, but it also gives confidence to investors looking to start data processing business in Mauritius, and ensures that data processors operating in Mauritius can provide these services to other signatory countries.

The legislative instrument that guides data protection in Mauritius is the Data Protection Act that was enacted by the National Assembly in 2004 with the aim of protecting the fundamental privacy rights of individuals against the use of data concerning them without their informed consent. The Act came into operation in February 2009. The Data Protection Office, a public office under the aegis of the Ministry of Technology, Communication and Innovation, is the primary data protection authority in the country. The Data Protection Commissioner, who heads the Data Protection Office, is responsible for the enforcement of the Act.

Within the context of the Data Protection Act, 'Personal data' means (1) data which relate to an individual who can be identified from those data, and (2) data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion. Sensitive personal data is defined under the Act as personal information concerning a data subject and consisting

[10] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=g57Ca9ut

[11] http://www.i-policy.org/2016/06/mauritius-joins-the-data-protection-convention-convention-108.html

of information pertaining to (1) racial or ethnic origin, (2) political opinion or adherence, (3) religious belief or other belief of a similar nature, (4) membership of a trade union, (5) physical or mental health, (6) sexual preferences or practices, (7) the commission or alleged commission of an offence, and (8) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The Data Protection Act requires that all data controller and data processor must register in writing with the Data Protection Commissioner, including amongst other things, (1) a description of the personal data being, or to be processed by or on behalf of the data controller, and of the category of data, (2) subjects, to which the personal data relates, (3) a description of the purpose for which the personal data is or will be processed, (4) a description of any recipient to whom the data controller intends or may wish to disclose the personal data, (5) the names, or a description of, any country to which the data controller directly or indirectly transfers, or intends or may wish, directly or indirectly, to transfer the data, (6) the class of data subjects, or where practicable the names of data subjects, in respect of whom the data controller holds personal data.

A data controller must not collect personal data unless it is collected for a lawful purpose connected with the function or activity of the data controller, and the collection of the data is necessary for that purpose. If the data controller collects personal data directly from the data subject, the data controller must at the time of collecting personal data ensure that the data subject concerned is informed of the fact that the data is being collected, the purpose or purposes for which the data is being collected, the intended recipients of the data, the consequences for that data subject if all or any part of the requested data is not provided, whether or not the data collected shall be processed and whether or not the consent of the data subject shall be required for such processing, and his right of access to, the possibility of correction of and destruction of, the personal data to be provided. Sensitive personal data cannot be processed unless the data subject has given his express consent to the processing of the personal data, or made the data public.

The above requirements will not apply to the processing of sensitive personal data if such processing is (1) necessary to (a) protect the vital interests of the data subject or another person, (b) for the performance of a contract to which the data subject is a party, (c) for compliance with a legal obligation to which the data controller is subject, (2) is required by any investigatory authority under the Financial Intelligence and Anti-Money Laundering Act, or (3) is required by law.

The Act provides that, personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data. The adequacy and the level of protection of a country shall be assessed in

the light of all the circumstances surrounding the data transfer, having regard in particular to (1) the nature of the data, (2) the purpose and duration of the proposed processing, (3) the country of origin and the country of final destination, (4) the rules of law, both general and sectoral, in force in the country in question, and (5) any relevant codes of conduct or other rules and security measures which are complied with in that country. The above data protection principle shall not apply where (1) the data subject has given his consent to the transfer, or (2) the transfer is necessary (a) for the performance of a contract between the data subject and the data controller, or for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller, (b) for the conclusion of a contract between the data controller and a person, other than the data subject, which is entered into at the request of the data subject, or is in the interest of the data subject, or for the performance of such a contract, or (c) in the public interest, to safeguard public security or national security. Finally, transfer is also allowed if it is made on 'such terms as may be approved by the Data Protection Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subject.'

2.4. Morocco:

Morocco has a robust data protection framework in place to protect the privacy, security and integrity of data in the country. Personal data protection is governed in Morocco by the Law n° 09-08 (passed 220) relating to the protection of individuals with respect to the processing of personal data and by its implementation Decree n° 2-09-165 passed in 2009.

Law n° 09-08 was important because its article 1.1 provided a clear definition of personal data in Morocco, as "any information of any nature and independently of its format, including the sound and images relating to an identified or identifiable individual, referred to in the Law as a 'concerned individual.' A person is deemed identifiable when he or she can be identified directly or indirectly, especially by reference to an identification number or one or several specific elements of his or her physical, physiological, genetic, psychological, economic, cultural or social identity." Additionally, article 1.3 defined sensitive data as 'any information pertaining to a 'concerned individual' that reveals racial and ethnic origin, political, philosophical, religious opinions or trade union affiliation, or that concern sex life or health, including the genetic data.'

The primary data protection authority in the country is the Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel ('CNDP') (in English 'National Control Commission for the Protection of Personal Data'), which is responsible for enforcing the Law.

As per the law, the processing of any personal data requires a prior notification to the CNPD. In contrast, the processing of sensitive data or of personal data that includes ID card numbers requires a prior authorisation from the CNDP. All applications – notification and authorization – require providing amongst other things, (1) the purpose(s) of processing the data, (2) the identity and the address of the data controller, (3) the personal data processed and the categories of persons about whom personal data are processed, (4) the time period for which the data will be retained, (5) the recipients or categories of recipients of the personal data, and (6) the measures taken to ensure the security of the processing. Additional specific security measures are required when processing sensitive data.

Similarly, the law also provides guidance to processors. Any personal data must be collected for specific, explicit and legitimate purposes and be subsequently processed in accordance with these purposes for which they are collected, and all personal data must be accurate, comprehensive and, when necessary, kept up to date. The processing of personal data shall have received the individual's consent unless it is required by the law, a contract, or a public service, or circumstances in which 'the processing relates to achieving a legitimate interest of the data controller, balanced against the interests and fundamental rights and liberties of the concerned individual.'

Critically for the purposes of our paper, the transfer of a data subject's personal data to another country is allowed only if the country provides a sufficient level of protection in relation to an individuals' private life and fundamental rights and liberties. The sufficient nature of the protection is evaluated with regards to national laws and applicable security measures. Data controllers may transfer personal data out of Morocco to countries that are not deemed to offer adequate protection if the transfer is necessary to (1) safeguarding the individual's life, (2) safeguarding the public interest, (3) comply with obligations relating to the recognition, exercise or defence of a legal right, (4) to the performance of a contract between the data controller and the individual, or pre-contractual measures undertaken at the individual's request, and (5) to the conclusion or the performance of a contract in the interest of the individual, between the data controller and a third party.

The entity processing the data must take all reasonable precautions with regard to the nature of the data and the risk presented by the processing, in order to preserve the security of the data and, among other things, to prevent third parties gaining unauthorised access to such data.

Violations of the obligations set forth in the Law are punishable as an administrative and/or criminal offence.

It is interesting to note that although the provision of the Law n° 09-08 will clearly protect the privacy and personal data of Moroccan citizens, its main driving objective is to facilitate the growth of the digital economy by encouraging foreign investment, including in the offshoring and business process outsourcing business. With 52,000 jobs and MAD 7.6 billion of turnover at the end of 2011, the Moroccan offshoring market is 5 times larger than South Africa's, and to 4 times the size of the Tunisian or Egyptian offshoring market[12]. The protection of personal data transfer was seen critical to creating trust in the legal framework and is therefore one of the conditions and drivers of the development of new technologies and of the digital economy in Morocco. Since 2009, when the law was passed, unsurprisingly, Morocco has been making efforts to have its level of data protections recognized by the EU in order to promote further international business and encourage foreign investment.[13]

2.5. South Africa:

In August 2013, the South African National Assembly passed the Protection of Personal Information (POPI) Bill, after more than four years of discussions and deliberations. In passing this bill, South Africa is preparing to fundamentally change the data privacy and protection environment for its citizens and business. The President promulgated the bill into law in November, although implementation of a large number of provisions in the act has not commenced yet, with broad expectation that the notification to this effect would come by end-2016.

The POPI Act is wide in its application and will, subject to certain exclusions, impact all persons processing personal information. European data protection practitioners will note that many aspects of POPI are based broadly on similar European legislation, including (1) the establishment of an Information Regulator to manage, monitor and enforce compliance, (2) a similar definition of Personal Data (referred to in POPI as Personal Information), and (3) the concepts of Data Subject, Data Processor (referred to in POPI as Operator), Processing and Data Controller (referred to in POPI as Responsible Party).

Additionally, the right data principles introduced in POPI are similar to the seven data protection principles referred to in European legislation. The right principles at the heart of POPI are:

1. Accountability – the Responsible Party is accountable for ensuring compliance
2. Processing Limitation – setting out the rules for how Personal Information will be processed lawfully, in a reasonable manner that does not infringe the privacy of the Data Subject and with

[12] http://www.lexology.com/library/detail.aspx?g=9bd21a58-fe63-4f20-8788-3a0dee604c66
[13] https://iapp.org/news/a/morocco-continues-efforts-to-obtain-european-commission-recognition-of-data-protection-level/

either the Data Subject's consent or in fulfilling certain other requirements such as the legitimate interest of the Data Subject

3. Purpose Specification – Personal Information must be collected for a specified purpose of which the Data Subject is aware
4. Further Processing Limitation – Further processing of Personal Information must be compatible with the purpose for which it was collected
5. Information Quality – The Responsible Party must take reasonable practical steps to ensure that the Personal Information is complete, accurate, not misleading and updated where necessary
6. Openness – The Responsible Party is required to notify both the Information Regulator and the Data Subject before it may process Personal Information
7. Security Safeguards – The Responsible Party is required to ensure the integrity of the Personal Information in its possession or under its control by implementing appropriate, reasonable, technical and organisational measures to prevent loss, damage or destruction of Personal Information or unlawful processing
8. Data Subject Participation – the Data Subject has the right to access and request information about his/her Personal Information held by a Responsible Party and require the Responsible Party to correct or destroy Personal Information

What distinguishes the situation after POPI with the past, when the interpretation of personal data was largely left to interpretation, is the precise and broadly-scoped definition of "Personal Information". Under POPI, Personal Information includes information relating to both an identifiable, living, natural person, and where applicable, an identifiable juristic person, and includes:

- information about a person's race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth;
- information relating to education, medical, financial, criminal or employment history;
- any identifying number, symbol, email address, physical address, telephone number or other particular assignment to the person;
- the blood type or any other biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

- the views or opinions of another individual about that person; and
- the name of the person, if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

The POPI Act allows a data subject the right to request that a responsible party correct or delete personal information that is inaccurate, irrelevant and excessive, or which the responsible party is no longer authorised to retain.

The primary government institution responsible for overseeing the execution and implementation of POPI is the Information Regulator, which has already been established under the law. In the performance of its functions, the Regulator is obliged to have due regard to and take account of (1) the information protection conditions, (2) the protection of all human rights and social interests which compete with the right to privacy (including the desirability of the free flow of information), (3) international obligations accepted by South Africa, and (4) developing international guidelines relevant to the protection of individual privacy. On the other hand, the critical role of the Information Protection Officer in public and private bodies who will be responsible for ensuring compliance of their organisation, and will liaise with the Information Regulator to ensure the act is implemented.

Under the POPI Act, personal information may only be processed if the data subject (or a competent person where the data subject is a child) expressly consents to the processing of the personal information, unless the exclusions with regard to consent apply. The consent of the data subject is not required where the processing of personal information (1) is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party, (2) complies with an obligation imposed by law on the responsible party, (3) protects a legitimate interest of the data subject, (4) is necessary for the proper performance of a public law duty by a public body; or (5)is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

Finally, and is most relevant to this paper, the POPI Act makes the transfer of Personal Information outside of South Africa subject to certain exceptions -- broadly determined by whether the transfer is in the best interest of the Data Subject or whether the Data Subject has consented. Critically. It requires the data recipient (in a foreign country) to be subject to a law or contract which (1) upholds principles of reasonable processing of the information that are substantially similar to the principles contained in the POPI Act, and (2) includes provisions that are substantially similar to those contained in the PPI Act relating to the further transfer of personal information from the recipient to third parties.

While the actual stringency with which POPI is implemented still remains to be seen, given that it has not come into force yet, it is expected that POPI will significantly increase the safeguards available to ordinary citizens and business. At the same time, however, it will significantly increase the administrative burden of companies of all sizes. Companies will need to invest in a number of areas including upgraded technologies, enhanced managerial skills, tighter processes to ensure consent of data subjects. The economic cost of this measures, and how they impact the economy at large is what we wish to aim to study in this paper.

3. Methodology:

The methodology for estimating the impact of data localization on the TFP and macro- economic indicators such as sectorial production, sectorial imports and sectorial exports was largely adopted from the paper " A methodology to estimate the costs of data regulations by Erik van der Marel, Matthias Bauer, Hosuk Lee Makiyama , and Bert Verschelde published in International Economics Journal, 2015.

The first step is to investigate the types of regulatory barriers to data flow in the various countries, in order to create the data regulation index for each country (Table 1). Then we got the data regulation index on a sectorial level using the data intensity adopted from the above mentioned paper (table 4).

Table (1)

Types of regulatory barriers in data services

Types of restriction	regulatory measure	outcome
Restrictions related to the foreign supply of data services	Is there a data localization requirement?	Yes/ limited/No
restrictions related ton internal productivity losses/admin costs	Is there a strict consent requirement for the collection, storage, dissemination of personal data?	Yes/No
	Does the law provide users with the right to review their stored information?	Yes/No
	Does the law provide users with the right to be forgotten/ deleted?	Yes/No
	Is a notification of breaches towards the government/user obligatory?	Towards government/user /government & user
	Are data protection impact assessments obligatory?	Yes/No
	Is a data protection officer required?	Yes/No/Qualified Yes
	Are there administrative sanctions for non-compliance? How height?	varies according to height of sanctions
	Does the government require easy access to companies' data?	Yes/No
	Are the companies required to retain data for a fixed period of time?	Yes/No

Source: E.Van der Marel et al. (2015)

This is followed by verifying what type of regulatory measures related to data are actually currently observed across a group of countries which have either proposed or already implemented data regulations. The actual laws for each country related to these data regulations as listed in Table2.

Table 2:

Selected economies and the pertaining laws for data localization:

Country	Title Pertaining Law for Data Localization
1.Egypt	Constitution, Cyber Crime Bill (Draft)
2.Morocco	Law n° 09-08, (dated February 2009), and Decree n° 2-09-165 (dated May 2009)
3.Kenya	Data Protection Bill 2013 (Draft), Kenya Information and Communications Regulations 2016, Cybersecurity Regulations (Draft)
4.Mauritius	Data Protection Act 2004
5.South Africa	Protection of Personal Information Act 2013

Table (3)

Survey of the existing data regulating laws in some selected African Countries:

	Weights by theme (bj)	Question weight (ck)	coding of data		outcome
Foreign supply of data services:	**0.3**		**NO**	**Limited**	**Yes**
Is there data localisation requirement?		1	0	3	6
Internal admin costs measures:	**0.7**		**No**		**Yes**
Is there a strict consent requirement for the collection, storage and dissemination of personal data		0.05	0		6
Does the law provide users with the right to review their stored information?		0.05	0		6
Does the law provide users with the right to forgotten, deleted?		0.047	0		6
			No	**Govt or user**	**Both**
Is notification of breaches towards the government and/or users obligatory?		0.2	0	3	6
			No		Yes
Are data protection impact assessments obligatory?		0.175	0		6
Is a data protection officer required		0.375	0		6
			NO	**Some**	**High**
Are there administrative sanctions for non-compliance? How much?		0.047	0	3	6
			NO		**Yes**
Does the government require easy access to companies' data?		0.047	0		6
Are firms required to retain data for a fixed period of time?		0.013	0		6
Country score (0-6)	∑j(bj) ∑k(ck) answer jk				

Note: Question weights are based on Christensen et al. (2013) and UK Ministry of justice (2012)

From the survey (Table 3) and interviews obtained in order to investigate the status of the regulations pertaining to data in each 5 countries: Egypt, South Africa, Morocco, Kenya , and Mauritius, we applied the formula obtained from (van der Marel E, et al., 2015) ∑j(bj) ∑k(ck) answer jk, to calculate the data regulation index DRL (3) for each of the above mentioned countries in 2007 in period (t).

Weights by theme (bj) and question weights (ck) were all obtained from the Christensen et al (2003), and UK Ministry of Justice (2012). Results of the calculated indexes are reported in Table **(4)**. Data

regulation index for Egypt is 1.152, for Morocco: 0.8148, Kenya: 0.7161, Mauritius: 4.4124, South Africa: 4.0635.

The obtained data indexes reveal that Mauritius is the country with the most laws and regulations governing the flow of data, followed by South Africa, Egypt by a lower extent and finally Morocco and Kenya with obvious lack of data regulations in the two last countries.

Table (4)

Index outcomes of the quantification method

	Egypt	Morocco	Kenya	Mauritius	South Africa
Foreign supply data services:					
Is there a data localisation requirement?	3	0	0	6	0
Internal admin costs measures:					
Is there a strict consent requirement for the collection, storage and dissemination of personal data?	0	6	6	6	6
Does the law provide users with the right to review their stored information?	0	6	6	6	6
Does the law provide users with the right to be forgotten or deleted?	0	6	0	6	6
Is notification of breaches towards the government and/or users obligatory?	0	0	0	3	6
Are data protection impact assessments obligatory?	0	0	0	0	6
Is a data protection officer required?	0	0	0	6	6
Are there administrative sanctions for non-compliance? How much?	0	6	3	0	3
Does the government require easy access to companies' data?	6	0	6	0	6
Are firms required to retain data for a fixed period of time?	6	0	0	0	0
Country scores (0-6)	1.152	0.8148	0.7161	4.4124	4.0635

Table 4 reflects the downstream linkage or indexes of downstream industry users of data obtained from (Van der Marel E, et al., 2015) Notice that some sectors are mode dependent on data than others. The data intensity for each downstream goods industry and services sector in a typical economy using Input – output tables from the U.S. Bureau of Economic Analysis (BEA).

Table (5):

Data Intensities

GTAP Sector	Sector description	Data intensity
Communication	Post and Telecommunication services	0.318
Obsict	Other business and ICT services	0.069
Fininsurance	Financial and Insurance services	0.050
Machinery	Machinery and Electronic equipment	0.049
Oconsumer	Other consumer services	0.048
Oservices	Public services, dwellings	0.040
Distribution	Trade and Distribution services	0.037
Water	Water and other Utility services	0.034
transport	Transport services	0.032
Construction	Construction	0.024
Othermanuf	Manufactures nec.	0.024
Fabmetals	Metal products	0.020
Nonmetmin	Mineral products nec.	0.014
Lumberpaper	Wood and Paper products	0.014
Energy	Coal, Petroleum and Gas production	0.011
Transequip	Motor vehicles and parts	0.008
Chemicals	Chemicals, Rubber and Plastic Products	0.008
Bevtextcloth	Beverages/tobacco products; Clothing and leather products	0.007
Metals	Ferrous metals and Metals nec.	0.007
Primagrother	Primary agricultural products	0.007
Procfood	Meat, Vegetable oils, Dairy, Sugar and Food products nec.	0.006

Source: Van der Marel E, et al., 2015)

Next we calculated the Data regulation indexes for 2 other periods, also called the augmented administrative data indexes (table 5). The Data Regulatory index DRL (1) is at t=0 or calculated in 2004 or the least restrictive scenario in terms of regulating the flow of data (i.e data services barriers have not been put in place). To augment the index for administrative barriers (t +1) a hypothetical time period when all the data regulation laws are moderately being implemented. (Van der Marel E, et al., 2015).

Finally, the third scenario period (t)where all regulatory barriers across all countries are being implemented.

The assigned weights in these 2 time periods are somewhat subjective and with lower weights according to expert judgment **(**van der Marel E, et al., 2015).

Table (6)

Data Regulations Indexes for periods (t=0) and (t+1) for augmented Index and the original index for period (t):

Country	Index (t=0)	Index (t+1)	Index (t)
Egypt	0.7	0.95	1.152
Morocco	0.4	0.5	0.8148
Kenya	0.3	0.6	0.7161
Mauritius	0.7	1.2	4.4124
South Africa	0.5	1.5	4.0635

Estimating Total Factor Productivity & Panel model estimation:

To estimate the macroeconomic impacts of movements in total factor productivity (TFP) as result of changes in data regulation policies, the study relies on the Global Trade Analysis Project (GTAP) model. The GTAP model is a multi-region, multi-sectorial computable general equilibrium model, which traces out the economy-wide impacts of policy shocks (Hertel, 1997). The model takes into account complex interactions between factor incomes and prices to trace out the impacts on sector output, GDP, trade and regional welfare. Changes in TFP, induced by data regulation policies are likely to have economy wide effects, since reductions in productivity may increase production costs throughout the whole economy and this may result in declines in factor income, industrial output and hence GDP. Our analysis relies on TFP measures obtained from imposing various data regulation scenarios as in tables (12) to (14). We first of all, estimate TFP for each sector and country using data on value added and the value of inputs used in each of the sectors. Since it is difficult to get TFP data for countries in Sub-Saharan Africa at the sector level, we use data from the GTAP database to get our TFP estimates. We use GTAP database for years 2004, 2007 and 2011. For output value added we used value of output at agent prices, and for inputs, we rely on value of inputs used/purchased in each sector. Following the standard approach in estimating total factor productivity (Solow, 1957; Van Beveren, 2012), a Cobb-Douglas production function is estimated, where value added of output in each sector, region and year is assumed

to be a function of the value of inputs used in each sector, region and year. A measure of TFP is obtained as residuals in the production function estimation. In the second step, a function relating TFP and data regulation policies is estimated. However, it should be acknowledged that our TFP estimates may not give a true reflection of the level of productivity in an economy because of the difficulties regarding getting the exact data on productivity. Our results from the general equilibrium modelling should be treated as indicative of what is likely to happen as a result of negative productivity shocks emanating from data regulation polices and the quantitative estimates are unlikely to be precise.

Estimating the **Total Factor Productivity for the countries under investigation on a sectoral level required estimating** data on value added for each sector and the value of inputs used in each of the sectors. We obtained data from the Global Trade Analysis Project (GTAP), because it provides data at a disaggregated level in terms of regions and sectors. Cobb-Douglas production function was estimated, where value added of output of each sector is assumed to be a function of the value of inputs used in each sector. We followed the standard approach in estimating total factor productivity (Solow, 1957; Van Beveren, 2012). A measure of TFP is obtained as residuals in the production function estimation.

Standard parametric estimation technique of data regulations on downstream TFP using the following equation.

Equation 1:

$$\ln (\mathrm{TFP})_{oit} = \alpha_i + \beta_1 \mathrm{DRL}_{oit} + \gamma_o + \delta_i + \zeta_t + \epsilon_{oit}$$

Equation (1)

The purpose of running the model is to obtain the elasticities, or the estimated coefficient of the (DRL).

Panel data set consists of 5 countries and 3 years for 15 sectors according to GTAP classification. Number of observations is 225. This is a balanced panel dataset. There were three fixed effect controlled for in the model namely for the country, sector, and year.

The output of the panel model estimation provides us with the elasticities, with the right sign, negative and statistically significant. (Table 6), for the data regulation index at period (t=0), and according to the obtained answers from the regulations survey in each country under investigation was estimated by the running the fixed effects model to be -0.00001. This reflects the negative impact of data regulation on TFP in the selected countries and the type of elasticity is inelastic since its absolute value is less than one in. The small value of the estimated elasticity compared the value of the estimated elasticity in the EU (-0.347), shows that the impact of data localization is less in the selected African

countries than the other set of EU countries which were examined the abovementioned paper. This is due to the fact and these are smaller economies with less linkages to the global economy and are less reliant on sectors that are heavy users of data. Thus the overall impact of data localization would not be as profound on TFP as it is the case in advanced economies.

In the (t+1) period, where most laws are moderately implemented, we have the effect on TFP remains statistically significant and negative. These sub-indexes allow us to augment the original index with administrative additional regulatory barriers and we notice that DRL(2) and DRL (3) the coefficients estimated are smaller than the DRL(1). Notice that these estimated coefficients become economically less significant is underscoring the fact that administrative barriers are only of high impact on the data related services. So, in order to capture the true impact of laws regulating the flow of data we will opt for the DRL(1) in the remaining analysis of this paper.

Table (7)

	Ln(TFP) at (t=0)	**Ln(TFP) at (t+1)**	**Ln(TFP) at (t)**
DRL (1)	-0.0000125* (0.0000065)		
DRL (2)		-0.00000335* (0.0000017)	
DRL (3)			-0.000000601 (0.00000337)
Observations	225	225	225
R-squared	0.2675	0.2669	0.266

Robust Standard error in parentheses

In order to overcome the problem of endogeneity, which entails that sectors that experience high TFP are the ones that lobby for lower regulations, that might be of concern in this model, the lagged values of the explanatory variables would be controlled for in the model represented by equation 1. We find that in DR(1) and DR(2), the elasticities are statistically significant with negative sign and are consistent with previous results. (Tables 7&8)

Table (8)

	LagLn(TFP) at (t=0)	LagLn(TFP) at (t+1)	LagLn(TFP) at (t)
DRL (1)	-0.0000386*		
	(0.518065)		
DRL (2)		-0.0000139*	
		(0.5173667)	
DRL (3)			-0.0000106
			(0.514499)
Observations	150	150	150
R-squared	0.28	0.28	0.27

Robust standard errors in parentheses

*** P<0.01

** P<0.05

* P<0.1

Macroeconomic Impacts

The model is an applied general equilibrium framework that imposes the conditions of producer and consumer maximization on the accounting framework of regional input-output data, and trade data (Hertel, 1997). The standard GTAP assumption is perfect competition and constant returns to scale, and bilateral trade is handled via the Armington framework, where products are differentiated by country of origin. The model assumes that there is a regional household that collects all income and allocates the income across private consumption, government, and savings according to a Cobb-Douglas utility function. Private household demand for commodities and services is assumed to be in constant difference elasticity form, whereas producer behaviour is assumed to have a constant elasticity of substitution production function. This model is used with the GTAP version 9 data base, with 2011 as the reference year, as well as 140 countries or regions and 57 sectors (Narayanan et al. 2012). The database represents the world economy linked through bilateral trade, transportation and trade protection. We aggregate the database into 15 sectors and 6 regions. We rely on the standard GTAP model and closure rules, which assume that all markets are in equilibrium, all firms earn zero pure profits, the regional household is on its budget constraint and there is full employment of resources. However, certain caveats have to be taken into account in this respect. Firstly, the assumption of full employment in most countries

in Sub-Saharan Africa considered in the analysis is likely to be unrealistic, since these countries have high rates of unemployment of unskilled labour. This is likely to have the effect of underestimating the impact of data regulation policies. Secondly, our general equilibrium model is static as opposed to a dynamic model, which captures investment impacts and year on year growth rates in output and trade, and this is also likely to underestimate the impacts of our policy shocks. However, we still rely on the static model, since the main objective of this paper is to highlight the costs of data regulation policies, without emphasizing on the role of investment and year on year growth rates.

Analysis in this paper is forward looking, as we project the world economy to 2016. **Over the period from our baseline of 2011 to 2016**, we assume that national real GDP, population, unskilled and skilled labour, capital, agricultural land, sectoral productivity, grow at exogenously set rates. From this projected 2016 database, changes in TFP scenarios as in tables (12) to (14) are simulated to evaluate the impacts on the overall economy, sector output and international trade.

Table (9) reflects the losses in TFP a consequence of data processing regulations for the year 2004, this was scenario 1 , in which we obtained the difference between ln TFP in 2011 (t+1) and ln TFP in 2004 (t=0),

Table (9)

TFP losses in percentage terms as a consequence of data processing regulations (Scenario 1), at (t=0)

Sector	Egypt	Morocco	Kenya	Mauritius	South Africa
Grains & Crops	-0.0008	-0.0003	-0.0006	-0.0005	-0.0004
Meat Lstk	-0.0004	-0.0003	-0.0005	-0.0004	-0.0005
Extraction	-0.0011	-0.0003	-0.0005	-0.0004	-0.0006
Text Wapp	-0.0009	-0.0004	-0.0006	-0.0004	-0.0005
Utilities	-0.0011	-0.0003	-0.0006	-0.0004	-0.0006
Other Services	-0.0114	0.0031	-0.0134	-0.0017	-0.0117
Manufacturing	-0.0240	0.0053	-0.0213	-0.0017	-0.0258
communication	-0.0012	-0.0004	-0.0005	-0.0004	-0.0010
Financial	-0.0012	-0.0004	-0.0005	-0.0004	-0.0008
Proc food	-0.0008	-0.0003	-0.0005	-0.0006	-0.0006
Construction	-0.0017	-0.0002	-0.0012	-0.0004	-0.0009
Business	-0.0030	-0.0005	-0.0015	-0.0004	-0.0039
Water	-0.0004	-0.0004	-0.0004	-0.0004	-0.0005
Transport	-0.0080	0.0005	-0.0052	-0.0008	-0.0065
Distribution	-0.0004	-0.0004	-0.0004	-0.0004	-0.0004

Note: sectors follow the GTAP classification

We notice that losses in TFP reflected in the table gives the consequences of the effects in the productivity of downstream industries when the data regulations have not been put into effect. (Scenario 1), or the least restrictive scenario. The findings reveal that the sector mostly affected is the construction in all the countries under study, and mostly in Morocco. These losses range from -0.0002% - 0.002% in Morocco and Egypt respectively.

The construction sector is the east sector impacted in terms of TFP loss as a result of data processing regulations in these scenarios. Construction sector is a less scalable sector (World Bank, WDR 2016) than other sectors such as retail with more complex products contacts which makes them more difficult to enforce. Thus the impact of ICT especially the internet and cloud computing is less evident and there is thus lower chance to reduce transaction costs or benefit from other synergies due to cloud computing in this sector

While sectors that rely heavily of the free flow of data such as banking and communication sectors have moderate loss in TFP. Particularly, losses in communication sector are the highest in South Africa 0.001% and least in Morocco and Mauritius at around 0.0004%.

In addition, we have to other scenarios where the regulations are set in the most restrictive manner in Scenario 3 and the moderate level in Scenario 2. Table 12 gives us the losses in TFP according to scenario 2 where we find that the same sector suffers the most from losses in TFP is the manufacturing sector across the five countries under study. Scenario 3 is the when all the regulations are implemented across all 5 countries and thus the largest loss in TFP in all sectors are found. (Table 11)

Table 10 reflects the changes in TFP a consequence of data processing regulations for the year 2007 , this is scenario 2, in which we obtained the difference between lnTFP in 2011 (t+1) and ln TFP in 2007 (t), see the results in table 10

Table (10)

TFP changes as a consequence of data processing regulations for data localisation (Scenario 2), at (t+1), moderately restrictive data regulation scenario

Sector	Egypt	Morocco	Kenya	Mauritius	South Africa
Grains & Crops	-0.0012	-0.0003	-0.0007	-0.0006	-0.0005
Meat Lstk	-0.0005	-0.0003	-0.0006	-0.0004	-0.0005
Extraction	-0.0019	-0.0003	-0.0006	-0.0004	-0.0006
Text Wapp	-0.0011	-0.0004	-0.0007	-0.0004	-0.0005
Utilities	-0.0014	-0.0003	-0.0007	-0.0004	-0.0006
Other Services	-0.0185	0.0044	-0.0172	-0.0029	-0.0150
Manufacturing	-0.0438	0.0076	-0.0290	-0.0031	-0.0354
communication	-0.0019	-0.0004	-0.0005	-0.0005	-0.0011
Financial	-0.0017	-0.0004	-0.0006	-0.0005	-0.0009
Proc food	-0.0011	-0.0003	-0.0005	-0.0007	-0.0006
Construction	-0.0032	-0.0002	-0.0017	-0.0004	-0.0013
Business	-0.0036	-0.0005	-0.0021	-0.0005	-0.0050
Water	-0.0004	-0.0004	-0.0004	-0.0004	-0.0005
Transport	-0.0134	0.0011	-0.0072	-0.0013	-0.0082
Distribution	-0.0004	-0.0004	-0.0004	-0.0004	-0.0004

Note: sectors follow the GTAP classification

Table 11 reflects the changes in TFP a consequence of data processing regulations for the year 2011 , this is scenario 3, in which we obtained the difference between lnTFP in 2011 (t+1) and ln TFP in 2004 (t=0), see the results in table 11

Table (11)

TFP changes as a consequence of data processing regulations for all data regulations (Scenario 3), at (t) : All regulatory barriers are applied across countries.

Sector	Egypt	Morocco	Kenya	Mauritius	South Africa
Grains & Crops	-0.0018	-0.0002	-0.0007	-0.0007	-0.0005
Meat Lstk	-0.0006	-0.0003	-0.0007	-0.0004	-0.0005
Extraction	-0.0026	-0.0003	-0.0007	-0.0004	-0.0008
Text Wapp	-0.0018	-0.0003	-0.0007	-0.0004	-0.0005
Utilities	-0.0018	-0.0003	-0.0009	-0.0004	-0.0006
Other Services	-0.0342	0.0058	-0.0232	-0.0036	-0.0221
Manufacturing	-0.0688	0.0115	-0.0434	-0.0036	-0.0478
communication	-0.0031	-0.0005	-0.0005	-0.0005	-0.0014
Financial	-0.0028	-0.0005	-0.0006	-0.0005	-0.0011
Proc food	-0.0017	-0.0003	-0.0006	-0.0008	-0.0007
Construction	-0.0047	-0.0001	-0.0022	-0.0004	-0.0016
Business	-0.0057	-0.0007	-0.0027	-0.0004	-0.0068
Water	-0.0004	-0.0004	-0.0004	-0.0004	-0.0006
Transport	-0.0221	0.0016	-0.0096	-0.0015	-0.0111
Distribution	-0.0004	-0.0004	-0.0004	-0.0004	-0.0004

Note: sectors follow the GTAP classification

Reflecting on the share of the construction sector in GDP in Morocco in 2004, 2007 and 2011 respectively, we notice the increase in its share of the GDP to reach 7.6% in 2008.

We notice that the other sectors rely more on data processing have significant changes in TFP in manufacturing where the changes in TFP reached (-0.03%) in South Africa in scenario (1);

(-0.04 %) in Egypt in scenario (2) and (-0.07%) in scenario (3). (tables 10&11). Bearing in mind that the share of manufacturing sector in GDP in South Africa is 30%and the share of manufacturing sector in GDP in Egypt is about 37%.

Finally, notice that the classification of the services sector in the World Bank (WDI) Database is different than the classification of the same sector in GTAP database.

Macro- Economic Impact using GTAP

In order to estimate the simulations for losses in GDP in the five African countries, We used exogneous variables to extrapolate the data to year 2020. Thus we projected the GTAP database to 2020, using GDP, population, labour force, productivity and capital endowment obtained from WDI database. The shocks are implemented, and econometric simulations performed using estimated coefficients from equation 2a, bearing in mind that data to GTAP sectors were aggregated so the results are easier adopted in the GTAP model estimations.

Notice that obtained simulations should be considered as indicative and not taken as an accurate estimates.

Ceterus Paribus, findings in table 15 disclose that losses exists in GDP when there are restrictions on the free flow of data in terms of laws and regulations that would impact the economic activities by as low as a decrease by 0.002 percent in Mauritius GDP in scenario (1) to as high as around 0.051% percent in South Africa's GDP in case of implementing the most restrictive scenario (3).

Results of the simulation exercise are presented in tables (12) to (15). Since data regulation policies are shown to reduce productivity, this is likely to increase production costs and this will have a negative effect on the overall economy. The impacts of restrictions on free flow of data on real GDP are shown in table 12, for the various scenarios considered. Overall, restrictions on data usage will result in real GDP declining for the economies considered, with the largest decline experienced by South Africa, followed by Egypt. The decline in GDP range from 0.002 percent in Kenya to high of 0.051 percent in South Africa, for all the scenarios considered. These results are largely driven by a decline in private consumption, for all regions except Morocco and Mauritius, where the decline in investment is driving the result. The decline in private consumption is in turn largely driven by a decline in quantity demanded by private households induced by a decline in per capita household income. An increase in production costs as a result of data regulation policies led to a decline in incomes due to increases in prices of goods. Results also show that South Africa will experience the greatest loss in terms of GDP decline. This may be driven by the fact that South African economy is heavily dependent on service sectors which are intensive on the use of data resources.

Table (12)

Simulation change results in real GDP

change at GDP	Scenario 1	Scenario 2	Scenario 3
Egypt	-0.014	-0.024	-0.040
Morocco	-0.005	-0.007	-0.010
Kenya	-0.012	-0.016	-0.022
Mauritius	-0.002	-0.003	-0.003
South Africa	-0.028	-0.037	-0.051

Looking at the impacts on real output (table 13), over the course of data regulation in 5 African countries under study, we notice that countries that were mostly impacted by changes in sectoral production include Egypt, Morocco, and Kenya where 10 out of 15 sectors had negative impact on production of these sectors due to data localization.

On the other hand, we find the least changes in sectoral production occurring in South Africa due to data localization. We notice that sectors that were adversely impacted by data localization laws include construction sector, which is the fastest growing sector in the selected African countries, in addition to the "other services sector", which includes the following subsectors: insurance, dwelling, recreation, Public administration, defence, health, and education. The manufacturing sector was also adversely impacted in the above mentioned tables.

Tables (14) and (15) presents results of the effect of data restrictions on international trade. Overall, results show a decline in imports in almost all of the sectors and regions considered. Imports are more prevalent in African countries because these countries altogether are net importers to goods and services. Thus the data localization regulations have the most significant impact on imports rather than exports.

Nevertheless, considering table 15, the country that was mostly negatively affected by data regulation was by and large Morocco compared to the other 4 African countries. On the sector level, manufacturing was the sector that mostly adversely affected by data regulations.

Table (13) Simulation results, changes in sectorial production

		Grains and crops	Meat Lstk	Extraction	Processed food	Text Wapp	Manufacturing	distribution	Utilities	Communication services	Business services	Financial services	water	transport services	construction	Other Services
Egypt	Scenario 1	0.013	0.005	0.006	-0.001	0.013	-0.046	-0.016	-0.013	-0.001	0.008	-0.007	-0.005	-0.004	-0.035	-0.016
	Scenario 2	0.023	0.010	0.010	-0.001	0.025	-0.084	-0.029	-0.024	-0.001	0.015	-0.012	-0.009	-0.007	-0.062	-0.028
	Scenario 3	0.037	0.016	0.017	-0.002	0.039	-0.132	-0.046	-0.037	-0.001	0.024	-0.019	-0.014	-0.012	-0.098	-0.048
Morocco	Scenario 1	-0.006	-0.004	-0.004	-0.006	-0.027	0.015	-0.004	0.003	-0.009	-0.007	0.002	-0.002	-0.001	0.019	0.004
	Scenario 2	-0.008	-0.006	-0.005	-0.008	-0.038	0.022	-0.006	0.004	-0.013	-0.010	0.002	-0.003	-0.002	0.028	0.006
	Scenario 3	-0.013	-0.008	-0.007	-0.012	-0.056	0.033	-0.008	0.006	-0.020	-0.015	0.003	-0.005	-0.002	0.042	0.009
Kenya	Scenario 1	0.007	-0.002	0.005	-0.002	0.016	-0.051	-0.012	-0.019	0.024	-0.003	-0.008	-0.013	0.005	-0.023	-0.019
	Scenario 2	0.009	-0.003	0.007	-0.003	0.022	-0.070	-0.016	-0.025	0.033	-0.005	-0.010	-0.017	0.007	-0.031	-0.025
	Scenario 3	0.014	-0.004	0.011	-0.004	0.033	-0.106	-0.024	-0.038	0.048	-0.007	-0.014	-0.025	0.012	-0.046	-0.034
Mauritius	Scenario 1	0.000	0.001	0.000	0.000	-0.004	-0.002	0.001	-0.001	0.000	0.001	0.000	-0.001	-0.001	-0.004	-0.002
	Scenario 2	0.001	0.003	0.000	0.001	-0.003	-0.005	0.002	-0.002	-0.001	0.002	0.000	-0.001	-0.001	-0.006	-0.003
	Scenario 3	0.001	0.003	0.000	0.001	-0.005	-0.005	0.002	-0.002	-0.001	0.003	0.000	-0.001	-0.001	-0.007	-0.004
South Africa	Scenario 1	0.053	0.006	0.013	0.009	0.031	-0.027	0.001	0.001	0.001	-0.010	0.009	-0.014	0.010	-0.087	-0.018
	Scenario 2	0.073	0.008	0.017	0.012	0.044	-0.037	0.002	0.002	0.002	-0.014	0.013	-0.019	0.013	-0.119	-0.023
	Scenario 3	0.098	0.011	0.024	0.017	0.059	-0.050	0.002	0.002	0.003	-0.019	0.017	-0.025	0.018	-0.161	-0.033

Table (14) Simulation results, changes in sectorial imports

		Grains and crops	Meat Lstk	Extraction	Processed food	Text Wapp	Manufacturing	distribution	Utilities	Communication services	Business services	Financial services	water	transport services	Construction	Other Services
Egypt	Scenario 1	-0.026	-0.024	-0.036	-0.016	-0.041	0.006	-0.038	-0.027	-0.029	-0.037	-0.055	-0.040	-0.014	-0.015	-0.015
	Scenario 2	-0.047	-0.042	-0.065	-0.029	-0.075	0.013	-0.069	-0.050	-0.052	-0.069	-0.098	-0.072	-0.025	-0.027	-0.029
	Scenario 3	-0.074	-0.067	-0.103	-0.045	-0.118	0.019	-0.110	-0.081	-0.083	-0.108	-0.155	-0.113	-0.040	-0.043	-0.040
Morocco	Scenario 1	0.014	0.021	0.011	0.012	0.000	0.002	0.003	0.011	0.014	0.013	0.015	0.032	0.014	0.024	0.009
	Scenario 2	0.020	0.030	0.016	0.018	0.001	0.003	0.005	0.016	0.020	0.018	0.021	0.046	0.020	0.036	0.014
	Scenario 3	0.030	0.045	0.023	0.028	0.001	0.004	0.007	0.024	0.030	0.028	0.032	0.069	0.031	0.054	0.023
Kenya	Scenario 1	-0.023	-0.024	-0.031	-0.045	-0.019	0.006	-0.030	-0.005	-0.055	-0.045	-0.060	-0.032	-0.032	-0.042	-0.028
	Scenario 2	-0.031	-0.026	-0.042	-0.061	-0.026	0.008	-0.041	-0.006	-0.074	-0.060	-0.081	-0.044	-0.043	-0.057	-0.038
	Scenario 3	-0.045	-0.034	-0.064	-0.090	-0.038	0.013	-0.060	-0.008	-0.108	-0.088	-0.119	-0.064	-0.064	-0.083	-0.058
Mauritius	Scenario 1	0.002	0.005	-0.002	0.001	-0.003	-0.002	-0.005	0.000	-0.002	-0.004	-0.003	-0.003	-0.001	-0.005	-0.001
	Scenario 2	0.003	0.006	-0.003	0.001	-0.004	-0.002	-0.008	0.000	-0.004	-0.006	-0.006	-0.003	-0.002	-0.007	-0.001
	Scenario 3	0.004	0.009	-0.004	0.002	-0.006	-0.003	-0.010	-0.001	-0.005	-0.007	-0.007	-0.005	-0.002	-0.009	-0.001
South Africa	Scenario 1	-0.041	-0.100	-0.003	-0.071	-0.090	-0.018	-0.004	-0.031	-0.082	-0.085	-0.095	-0.112	-0.069	-0.137	-0.087
	Scenario 2	-0.056	-0.137	-0.004	-0.098	-0.124	-0.025	-0.005	-0.042	-0.112	-0.116	-0.130	-0.153	-0.095	-0.187	-0.120
	Scenario 3	-0.076	-0.186	-0.005	-0.133	-0.168	-0.034	-0.008	-0.058	-0.152	-0.157	-0.176	-0.207	-0.129	-0.253	-0.159

Table (15) Simulation results, changes in sectorial exports

		Grains and crops	Meat Lstk	Extraction	Processed food	Text Wapp	Manufacturing	distribution	Utilities	Communication services	Business services	Financial services	water	transport services	construction	Other Services
Egypt	Scenario 1	0.073	0.108	0.039	0.052	0.119	-0.099	0.033	0.025	0.095	0.085	0.099	0.141	0.037	0.025	0.031
	Scenario 2	0.132	0.199	0.070	0.094	0.216	-0.184	0.061	0.046	0.171	0.158	0.179	0.253	0.068	0.043	0.063
	Scenario 3	0.210	0.318	0.112	0.149	0.340	-0.286	0.099	0.076	0.270	0.249	0.283	0.402	0.105	0.070	0.081
Morocco	Scenario 1	-0.023	-0.047	-0.012	-0.023	-0.042	0.023	-0.017	-0.016	-0.026	-0.021	-0.023	-0.054	-0.016	-0.013	-0.006
	Scenario 2	-0.034	-0.068	-0.017	-0.033	-0.059	0.033	-0.024	-0.023	-0.038	-0.031	-0.034	-0.078	-0.023	-0.018	-0.010
	Scenario 3	-0.050	-0.100	-0.026	-0.049	-0.087	0.049	-0.034	-0.033	-0.058	-0.047	-0.051	-0.116	-0.034	-0.028	-0.019
Kenya	Scenario 1	0.060	0.115	0.051	0.078	0.062	-0.090	0.027	-0.023	0.097	0.080	0.093	0.075	0.030	0.053	0.019
	Scenario 2	0.081	0.157	0.069	0.106	0.086	-0.122	0.037	-0.032	0.132	0.107	0.127	0.102	0.040	0.071	0.030
	Scenario 3	0.119	0.230	0.100	0.156	0.127	-0.186	0.055	-0.048	0.193	0.159	0.186	0.149	0.061	0.104	0.051
Mauritius	Scenario 1	0.001	0.006	0.009	0.004	-0.005	-0.001	0.009	-0.002	0.004	0.006	0.005	0.006	0.000	0.004	0.000
	Scenario 2	0.002	0.011	0.016	0.007	-0.004	-0.006	0.016	-0.001	0.007	0.010	0.008	0.012	0.000	0.007	0.000
	Scenario 3	0.001	0.013	0.019	0.008	-0.006	-0.006	0.020	-0.001	0.008	0.013	0.011	0.014	0.000	0.009	-0.001
South Africa	Scenario 1	0.106	0.197	0.018	0.134	0.228	-0.031	0.009	0.058	0.162	0.153	0.180	0.210	0.121	0.095	0.131
	Scenario 2	0.145	0.271	0.024	0.184	0.314	-0.044	0.014	0.080	0.221	0.211	0.247	0.287	0.167	0.130	0.182
	Scenario 3	0.196	0.367	0.033	0.249	0.426	-0.059	0.020	0.110	0.300	0.285	0.334	0.390	0.226	0.176	0.238

4. Conclusion and Policy Recommendations:

The current research paper reaches the conclusion that fighting the trend of data nationalization is crucial since it hinders the necessary and essential role of the global trade in realizing economic development. According to the UNCTAD, 107 countries had privacy laws or bills, but only 51 of them were developing countries.

The advent of the Internet and new storing technologies such as cloud computing, enables half of the global trade. The momentum of ICT on global trade results in cheaper and improved services. Modern businesses find cloud computing cost effective and economically worthwhile that more than 60 percent of the world's servers' workloads now take place on cloud servers, up from 8 percent five years ago.

It is clear from the findings of this paper that laws that stipulate certain data to be stored inside the borders of where the data originated, will increase the costs for financial services firms, and the firms will have to pass those costs on to the businesses and customers that they serve. The need to protect citizens and their sensitive information is completely understood, and in the days of security fears across the world, is a fair concern for governments. However, the strategy to ensure that should include a wide range of policy tools, out of which data-flow restrictions is the least effective and most costly policy option. It is the proverbial blunt knife that hurts more than it helps. Instead of restricting data-flows, governments should enact data protection laws that differentiate between types of data and then enact protections that are appropriate to that type or class of data (data classification).

Recommendations to policy maker include the urgency to harmonize interoperability of data protection regimes across regions for starters. This would result in a surge in the cross border data flow and decrease the probability of data nationalization.

This would eventually stimulate economic growth and development which is the main aim developing countries such as African countries under study in this research paper.

References

Allen and Overy, (2012) Less than adequate – cross-border data transfers under the proposed Regulation,

Barry, Renee and Matthew Reisman (2012), Policy Challenges of Cross-Border Cloud Computing, United States International Trade Commission, Journal of International Commerce and Economics. https://www.usitc.gov/journals/policy_challenges_of_cross-border_cloud_computing.pdf

Bauer, M., F. Erixon, M. Krol, H. Lee-Makiyama, with B. Verschelde, 2013. "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce." European Centre for International Political Economy (ECIPE), March. Brussels: ECIPE for the US Chamber of Commerce. Available at. https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel, Bert Verschelde (2014), The Costs of data Localisation: Friendly Fire on Economic Recovery, ECIPE Occasional Paper No. 3/2014 European Center for International Political Economy, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

Bauer, M., H. Lee-Makiyama, E. van der Marel, and B. Verschelde (2014). "The Costs of Data Localisation: Friendly Fire on Economic Recovery." ECIPE Occasional Paper 3/2014. Brussels: ECIPE. Available at www.ecipe.org/app/uploads/2014/12/OCC320141.pdf.

Castro, Daniel, The False Promise of Data Nationalism, Info. Tech. & Innovation Found. 1 (Dec. 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf

Federal Trade Commission, 2012, Protecting Consumer Privacy in an Era of Rapid Change. Available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Hertel, T. W. (1997). *Global Trade Analysis: Models and Applications.* Cambridge University Press.

Kuner, Christopher (2012), Data Nationalism and Its Discontents, Emory Law Journal Online, Retrieved from: http://law.emory.edu/elj/elj-online/volume-64/responses/data-nationalism-its-discontents.html

Leber, Jessica, Big Oil Goes Mining for Big Data, MIT Tech. Rev. (May 8, 2012), http://www.technologyreview.com/news/427876/big-oil-goes-mining-for-big-data/

Matthieu Pélissié du Rausas et al., McKinsey Global Inst., Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity 22 (2011), available at http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

Michael Rosenwald (2011), Cloud centers bring high-tech flash but not many jobs to beaten-down towns, Washington Post. Available at: https://www.washingtonpost.com/business/economy/cloud-centers-bring-high-tech-flash-but-not-many-jobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_story.html

Mihaylova, Iva, Could the Recently Enacted Data Localization Requirements in Russia Backfire? (July 11, 2015). U. of St. Gallen Law & Economics Working Paper No. 2015-07. Available at SSRN: http://ssrn.com/abstract=2629533 or http://dx.doi.org/10.2139/ssrn.2629533

Miroudot, S., R. Lanz and A. Ragoussis (2009), Trade in Intermediate Goods and. Services, OECD Trade Policy Working Papers, No. 93.

Narayanan, B., Aguiar, A., & McDougall, R. (. (2012). *Global Trade, Assistance, and Production: The GTAP 8 Data Base.* West Lafayette: Center for Global Trade Analysis, Purdue University. Retrieved from www.gtap.agecon.purdue.edu/databases/v8/v8_doco.asp

Palmisano, Samuel, (2006), The Globally Integrated Enterprise, Foreign Affairs, May/June 2006 Issue retrieved from https://www.foreignaffairs.com/articles/2006-05-01/globally-integrated-enterprise

Schiff, Aaron, (2015)DATA DRIVEN INNOVATION IN NEW ZEALAND. Available at http://www.innovationpartnership.co.nz/wp-content/uploads/2016/07/Data-Driven-Innovation-in-New-Zealand.pdf

Sáez, Sebastián; Taglioni, Daria; van der Marel, Erik; Hollweg, Claire H.; Zavacka, Veronika. 2014. Valuing Services in Trade : A Toolkit for Competitiveness Diagnostics. World Bank, Washington, DC. © World Bank. https://openknowledge.worldbank.org/handle/10986/21285 License: CC BY 3.0 IGO.

Solow, R. M. (1957). Technical change and the aggregate production function. *Review of Economics and Statistics*, 312-320.

Van Beveren, I. (2012). TOTAL FACTOR PRODUCTIVITY ESTIMATION:A PRACTICAL REVIEW. *Journal of Economic Surveys*, 98-128.

Van der Marel. E. (2015) Disentangling the Flows of Data: Inside or Outside the Multinational Company? ECIPE OCCASIONAL PAPER • 07/2015, http://ecipe.org/app/uploads/2015/07/ECIPE-Data-Flows-final.pdf

Wooldridge, Jeffrey M. 2002. *Econometric analysis of cross section and panel data*. Cambridge, Mass: MIT Press.

Burfisher, M.(2011) "Introduction to Computable General Equilibrium Models", Cambridge University Press.

Bauer, M., F. Erixon, M. Krol, H. Lee-Makiyama (2013) "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce", ECIPE / US.

Costinot A.Ontheoriginsofcomparativeadvantage.JIntEcon2009;77(2):255–64.

ECIPE. The economic importance of getting data protection right: protecting privacy, transmitting data, moving commerce. ECIPE, Brussels.

Fouré J, Benassy-Quere A, Fontagne L. The great shift: macroeconomic projections for the world economy at the 2050 horizon, CEPII. Working paper 2012-03; 2012.

JorgensonDW,HoM,SamuelsJ.InformationtechnologyandUSproductivitygrowth:evidencefromaprototypeindustryproductionaccount.In:MassM,StehrerR,editors.IndustrialproductivityinEurope:growthandcrises.USA:EdwardElgar Publishing; 2010.p.35–64.

Kommerskollegium (2014) "No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies Based in Sweden", Kommerskollegium, 2014:1, National Board of Trade.

Lisenkova, K., M. Merette and R.E. Wright, 2011, "Demographic Applications of OLG-CGE Modelling", Journal of Economic Surveys (in submission).

Ian Sue Wing, Computable General Equilibrium Models for the Analysis of Energy and Climate Policies

Ken Pearson and Mark Hirridge, 2005, Hands-on computing with RunGTAP and WinGEM to introduce GTAP and GEPPACK

Thomas W. Hertel, 2010, Global trade analysis Modelling and applications.

World Bank Group. 2016. World Development Report 2016 : Digital Dividends. Washington, DC: World Bank.

Websites:

World Bank: http://www.worldbank.org/

UNCTAD: http://unctad.org/en/Pages/Home.aspx

Global trade analysis project (GTAP): https://www.gtap.agecon.purdue.edu/

GEMPACK: http://www.copsmodels.com/gempack.htm

Appendix

Figure 1:Real GDP values (Million $) of the selected 5 countries

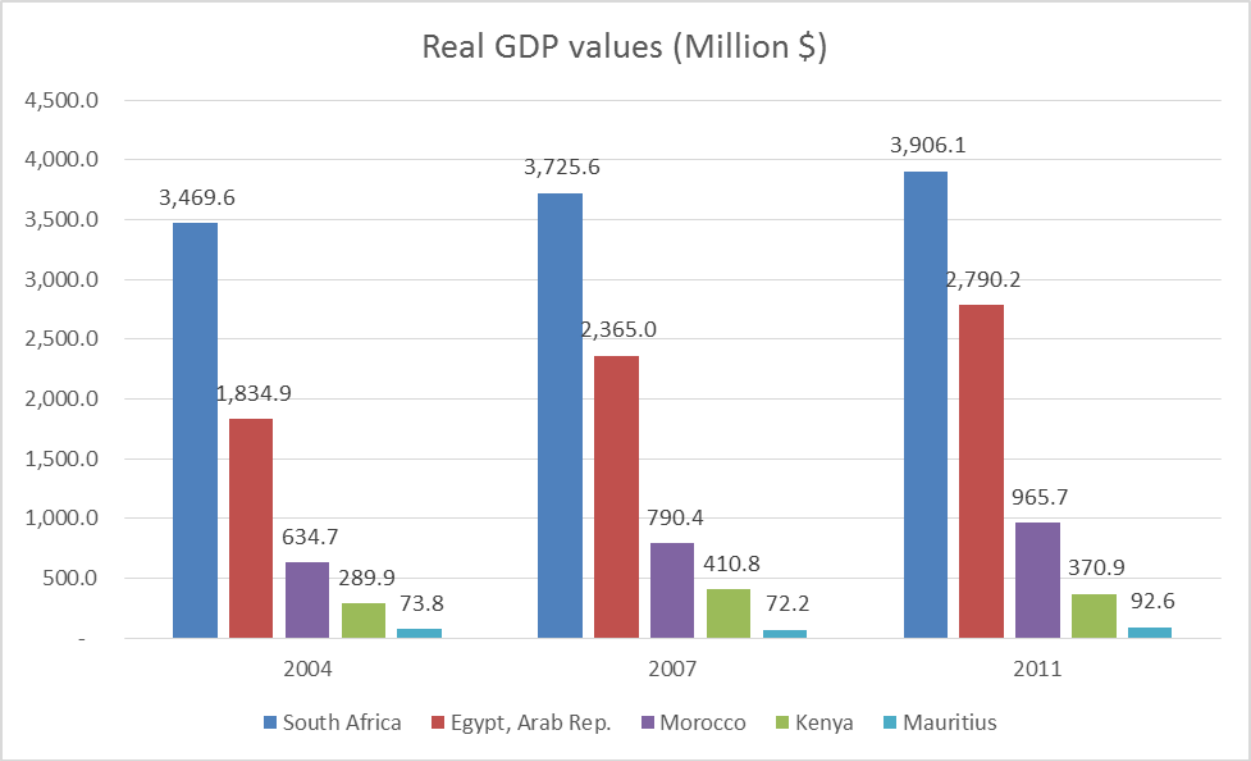


Figure2: Trade Balance of the selected 5 countries