

A dark blue vertical bar runs down the left side of the slide. A blue arrow points to the right from this bar, containing the date.

14 April 2021

# Impact of Local and Global Regulations

Several thin, curved lines in dark blue and light grey originate from the bottom left and sweep upwards and to the right.

Leilah Collier  
Nkagisang Mere  
Pfano Matsheketsheke  
Tiree Conochie  
GROUP ZF

## **Introduction**

Electronic commerce, described broadly as the purchase of items or services over the internet, is effectively changing the value chain and structure of the retail industry. It enhances horizons for retailers and suppliers globally to access consumers across vast geographical contexts, including international borders while increasing the range of products available for consumers. However, this incurs a consequent effect on a range of regulations including data protection, trade, competition policy, taxation and protection of intellectual property. On the one hand, e-commerce provides an opportunity to open retail markets for smaller scale suppliers, but on the other, the interactions of e-commerce with data and fundamental economies of scale can lead to market dominance by larger providers and affirm patterns of trade that favor companies and countries that were early innovators. E-commerce can offer companies an opportunity to undermine local producers by avoiding tax and conventional regulations, thus countries, including South Africa have adjusted and are enacting several policies that shape and impact how the e-commerce environment operates.

This paper will unpack key regulatory approaches taken by South Africa that impact how local and international e-commerce businesses operate in the country, followed by an assessment of how market leaders like Alibaba and Amazon have been affected by regulatory measures around the world. Lastly, policy recommendations will be given, that can have a positive impact on ecommerce growth.

### **South Africa's data protection, cross-border data flows, data localization, and cybersecurity laws impacting the e-commerce environment.**

Data protection laws ensure the security and integrity of consumers personal information online (Badran, n.d.). It is critical that sensitive information remains secure, protected, and only used in specifically stated ways to prevent unlawful usage – banking scams, identify fraud etc. Additionally, businesses could process this information for non-statistical purposes to gain an upper hand over the competition (Badran, n.d.; Presidency, 2013; Presidency, 2002). Government also needs to ensure the digital framework is secured from a range of threats – foreign powers, terrorists, and criminals (Sutherland, 2017). If stringent data protection laws are not enacted, the trustworthiness for the e-commerce environment diminishes, as consumers will prefer the brick-and-mortar approach.

South Africa's Protection of Personal Information Act (POPI), Electronic Communications and Transaction Act (ECT), alongside the National Cybersecurity Policy Framework (NCPF) and Consumer Protection Act enacts laws, policies, and regulatory bodies to offer more power and protection to consumers over their personal information and digital interactions. The Information Regulator oversees the responsibility for the implementations, executions, and compliance of public and private bodies collecting and processing personal information to adhere to law and good practices (Badran, n.d.; Presidency, 2013; Presidency, 2002). It is noted, the POPI reflects many aspects of the EU Data Protection Directive encompassing data protection and privacy laws, forming a basis for international standards (Badran, n.d.). Therefore, promoting the capabilities of data imports and exports between countries of similar data protection laws.

Although, data protection laws with regards to cross-border data flow laws, majorly impact an array of sectors (Badran, n.d.). Cross-border data flow laws restrict the transfer of data to countries which lack sufficient data protection therefore, businesses are severely affected in foreign jurisdictions. However,

exceptions are commonplace for cross-border data transfers adhering to performance of contracts, legalities, or for the benefit or protection of data subjects (Tesfachew, 2016). POPI includes these exceptions, in addition to binding rules – an entity is subject to law of sufficient data protection (Presidency, 2013). Consequently, enabling free data movement, transparency, oversight, and surety of data protection. However, approval processes are costly (Badran, n.d.; Tesfachew, 2016).

Currently, South Africa has no data localization laws – personal data is required to be retained within the original jurisdiction (Tesfachew, 2016). In general, data localization significantly impacts trade, innovation, and competition (Badran, n.d.; Tesfachew, 2016). This is to mitigate security risks in foreign jurisdictions and reduces the dominance of internet services from foreign countries (Tesfachew, 2016). Indonesia and Russia have adopted such laws whereby, businesses experience compliance burdens (Tesfachew, 2016). Therefore, alongside cross-border data flow laws, South Africa encourages e-business investment, given the safeguards are adhered to.

Furthermore, NCPF ensures the security of the cyberspace at national, provincial and municipal governments (Mahlobo, 2012). The framework sources its strategies from the EU, NATO, and the USA, which are more advanced users of digital technologies and have faster policy formation (Sutherland, 2017). In addition, the ECT supported with the POPI permits powers to cyber inspectors to investigate and access computer and network systems that are potentially unlawful therefore, providing legal framework for public, private, individual, and corporates (Presidency, 2002; Presidency, 2013). However, South Africa's implementation of cyber policies are slow, owing to poor service delivery, outdated infrastructure, and lack of technical skills. Additionally, no cyber inspectors were appointed, and no offences were prosecuted (Sutherland, 2017).

Effectively, South African laws and regulations are sound on paper, encouraging e-business activity, given that businesses operating within jurisdiction adhere to laws and regulations. In addition, businesses from foreign jurisdictions importing South African data must reflect data protection and privacy laws, otherwise administrative fees become costly. However, the delays, inefficient implementations, and lack of education of cyber policies offer holes for criminals to exploit therefore, hindering the consumer trust for the South African e-commerce environment.

### **South Africa's e-commerce taxation and credit laws, and regulatory impact on customer demand**

Taxation laws outlined in the Income Tax Act (ITA) and amendments to the VAT Act enacted in 2014 have been aimed at leveling the playing field between local and foreign suppliers. Prior to this, local suppliers were formally required to include tax on sales, while foreign suppliers were not, allowing them to undercut local suppliers (Graeme Palmer, 2014). The regulations require that e-businesses supplying e-services to South Africans where payment originates from a South African bank to register as VAT vendors paying a standard rate of 14% and small-scale importers are required to register for an "import code" should they exceed a R50000 transaction threshold within a month (Bardopoulos, 2015). However, it has been suggested that the current taxation system is not streamlined, and thus discourages small scale e-commerce, while reducing any efficiencies related to it (Anthea Paelo, 2019).

When it comes to business-to-business (B2B) e-commerce, credit lines are often expected, with most B2B customers requiring the purchases of goods on a credit line in order to manage their finances at scheduled

times (Nathan Orr, 2020). The National Credit Act regulates pre-contract disclosure, credit agreements and post-contractual information, while conferring certain rights to consumers regarding withdrawal from credit agreements and early settlements, with Section 75 covering joint and several liability. By regulation, any e-business providing any form of credit to South African consumers requires licensing from the Office of Fair Trading, which requires forces them to have fair and non-discriminatory terms and conditions for consumer credit.

On the demand side, broadband data prices have been the biggest barrier of entry for many South Africans and SMEs, despite a mandatory data cost slash issued by the competition commission in 2019. A draft document published by ICASA, called the Mobile Broadband Services Regulations 2021, read with section 4 of the ECT act outlines regulations meant to provide relief to consumers in terms of retail prices, ensuring that consumers pay affordable rates (ICASA).

### **Comparing Regulation of E-Commerce Leaders: Amazon and Alibaba**

Big Tech companies are under increased scrutiny by regulatory bodies. The Federal Trade Commission (FTC) is a federal agency in the United States tasked with protecting consumers and promoting competition. The FTC develops policy and collaborates with law enforcement to advance consumer protection and competition. Consumer protection is achieved by stopping unfair, deceptive or fraudulent practices in the marketplace. Competition consists of price, selection and service. The FTC seeks to protect and advance competition in the US by enforcing antitrust laws. (Federal Trade Commission, n.d.). Antitrust laws are statutes developed by governments to protect consumers from predatory business practices and ensure fair competition. Similarly, in China, the State Administration for Market Regulation (SAMR) is responsible for market regulation, including creating a market environment of fair competition (National Institute of Metrology, China, 2013). The European Union has the European Commission as its governing body. They have been known to play an active and aggressive role in e-commerce regulation. In 2000, the regulatory bodies of the EU devised the e-Europe Action Plan which called for creating a comprehensive legal environment to legislate and enforce European ecommerce guidelines. (Brandom, 2020)

Amazon currently operates in the US and the EU. Both regions have brought antitrust charges against Amazon and have launched investigations. (Palmer, 2020) The regulatory bodies are concerned about the growing power of Amazon and its potential to be classified as a monopoly. A monopoly can decide the price of products and will be able to sell without competition, meaning that they could raise prices at will. Their investigations are around allegations that Amazon uses third-party seller data to create their own products (Bishop, 2020). A ruling with respect to such an allegation may break Amazon up into different sites, preventing them from being both a manufacturer and operator of the platform. Amazon had recently made changes to their third-party seller service, giving more legal options to sellers, in response to a separate investigation by German regulators. These include better protections for businesses – Amazon must notify sellers, within 30 days, before removing them from the platform and include reasons for removal. They now also allow sellers to take Amazon to court in their own countries. (Brandom, 2020)

Alibaba was also recently at the centre of an antitrust and anti-monopoly violation investigation. The Ant Group, a subsidiary of Alibaba, underwent a major revamp after new antitrust rules went into effect in February 2021 (Zhang, 2021). Alibaba was also accused of alleged monopolistic practices, such as forcing merchants to sell exclusively on their site (Jennings, 2020). China is leaning into antitrust regulation in order to stay competitive with the US. The Chinese government views antitrust laws as a powerful tool,

not only for combating monopolistic practices, but also to achieve broader policy objectives. These could include maintaining price stability and improving technological infrastructure. (Zhang, 2021)

What this all means for ecommerce: E-commerce companies service a large consumer market. As such, the goals of the regulatory bodies to protect consumers are enacted by enforcing the antitrust regulations against the likes of Amazon and Alibaba. When customers feel that they are being protected and have options when it comes to ecommerce, ecommerce can continue to grow. As for the promotion of competition, antitrust regulation ensures that ecommerce leaders like Amazon and Alibaba do not hold monopoly power over sellers. These regulations have started including the protection of third-party sellers on these types of platforms as well.

#### WHAT GLOBAL AND LOCAL REGULATIONS SHOULD BE AVAILABLE:

Similar to the United States's FTC and China's SAMR, the Competition Commission of South Africa is empowered by the Competition Act to act as the regulatory body for business practices in South Africa (Competition Commission South Africa, 2021). They have recently initiated an inquiry into online intermediation platforms that operate in South Africa, both local and international platforms, in which they will investigate the trends of these platforms which includes, but is not limited to, the monopoly/bullying practices such as exclusive contracting and price setting (competition commission South Africa, 2021). This shows that even in the preliminary stages of e-commerce in South Africa, it would still be difficult for SME's that are not subsidiaries of larger companies to "successfully" enter the e-commerce market. Although the recent rules to tax cross-border e-commerce transactions have closed price gaps between local and international service providers, there are still price gaps due to the "support" behind the international platforms.

#### Regulating the sale price of goods of international e-commerce platforms:

In cases where e-commerce platforms are supported by large companies, that platform can afford to lower their prices to mitigate competition. In some cases, it does benefit the economy when prices are lowered due to high competition, but in cases where it is done to create a barrier of entry it will later lead to a monopoly of that platform (natural monopoly). Below are two snippets of how e-commerce platforms supported by large companies can lower their prices (using Mr D Food and Uber Eats as examples)

#### McDonald's

- Uber Eats delivery fee – R10
- Mr D Food service fee – R5

Menu Item	Mr D Food	Uber Eats
Big Mac Meal	R53.90	R59.90
McFeast Meal	R94.90	R93.50
Chicken Foldover Meal	R78.00	R70.90
Double Quarter Pounder Meal	R84.90	R84.90
Grand Chicken Meal	R78.90	R79.90
Cheese Burger	R28.90	R38.50
Hamburger	R25.90	R36.00
Average Price	R63.63	R65.37

Prices of McDonald's meals on different platforms in 2019 (Jamie McKane, 2019)

## McDonald's

Delivery Fee:

- Uber Eats – R3
- Mr D Food – R5

Menu Item	Mr D Food	Uber Eats
Big Mac	R47.90	R46.43
McChicken Meal	R51.90	R52.94
Quarter Pounder with Cheese	R58.90	R58.82
Big Mac Meal	R59.90	R55.15
McFeast Spicy Meal	R103	R93.41
Beef Sharebag	R231.90	R218.04
Chicken Sharebag	R231.90	R220.04
Average Price	R112.20	R106.40

Prices of McDonald's meals on different platforms in 2020 (Jamie McKane, 2020)

In 2019 we see that Mr D Food had a lower average price for McDonald's meals and lower delivery fees than Uber Eats, but we see that in 2020 Uber Eats was able to drop their prices in order to compete with Mr D Food. Suppose that this trend continues, in the case where an SME platform would like to join this market, it would be difficult to penetrate the low costs offered by the "giants" at the same point of quality offered by them.

Regulating prices would give room for SMEs to enter the market. This has recently been done in India using Foreign Direct Investment (FDI) regulation to remedy e-commerce platform power in retail competition. Amongst other restrictions they have restricted e-commerce entities from influencing prices. (Paolo, 2019).

### Regulating against discrimination:

There has been a massive growth in e-commerce as the South African lockdown restrictions have acted as a massive accelerant in pushing South Africans further in purchasing goods and services online (Thenga, 2020). This has led to more businesses integrating to the online platform as well as many SME's starting as an e-commerce. However, not every South African has been given equal access to benefit from this growth, many of these online retailers have restricted deliveries to specific areas in the country.

With the already existing South African e-commerce giants such as Zando either delivering to specific areas or charging a surplus on deliveries to remote areas, and large South African retailers such as Pick n Pay and Woolworths following the lead with similar restrictions. This means that a certain demographic of people do not have access to the benefits of e-commerce furthermore they will not have access to these benefits as no law requires online retailers to not discriminate according to class (classism). Areas that have extremely "poor infrastructure" (rural areas) do not have access to these services as online retailers have excluded them in the list of area they deliver to or charge a surplus on delivery fees (a percentage higher than the original delivery fee calculated by distance). This does not benefit the entire population, nor does it enhance economic inclusion but perpetuates the exclusion.

A law is required to ensure that online retailers that do have the resources to deliver to rural areas do in fact deliver to those area at the standard delivery rate fee.

In conclusion, South Africa's lawful and regulatory framework pertaining to e-commerce is substantially sound. Reflecting the strategies of forerunners and advanced users of digital frameworks, South Africa has a strong basis to promote local and international e-commerce. However, the soundness of the POPI, ECT, NCPF, Consumer Protection Act, ITA, National Credit Act, Competition Act and the powers enabled to regulatory bodies are irrelevant if government lacks the execution. Furthermore, the increased scrutiny on global e-business leaders to prevent monopolies, protect consumers & SMEs and promote SME growth. There is considerable room for improvement to South Africa's e-commerce environment – producing a sufficient supply of skilled technicians to build and maintain infrastructure; more accountability for government and regulatory bodies; more coordination between governmental levels, the public and businesses; an increased drive towards education; and equitable access to digital infrastructure. Overall, every South African should benefit from this growing e-economy or at least be provided the opportunity.

Reference list:

Competition Commission South Africa (2021) Competition Commission South Africa Available at: <https://compcom.co.za> (Accessed 5 April 2021)

Competition Commission South Africa, 2021. Online Intermediation Platforms Market Inquiry Terms of Reference Draft for Public Comment, South Africa

Goga S. Paelo A., 2019, Issues in the regulation and policy surrounding e-commerce in South Africa, University of Johannesburg Centre for competition regulation and economic development, South Africa.

McKane J., 2020. Uber Eats vs Mr D Food – The cheapest food delivery app in South Africa (mybroadband.co.za). Available at: <https://mybroadband.co.za/news/it-services/366084-uber-eats-vs-mr-d-food-the-cheapest-food-delivery-app-in-south-africa.html/amp>, South Africa

McKane J., 2019. Uber Eats vs Mr D Food – 2019 pricing shootout (mybroadband.co.za) Available at: <https://mybroadband.co.za/news/technology/326191-uber-eats-vs-mr-d-food-2019-pricing-shootout.html#:~:text=Uber%20Eats%20charges%20a%20variable%20delivery%20fee%20depending,of%20meals%20from%20a%20selection%20of%20popular%20restaurants.,> South Africa

National Credit Act No.34, 2005, Section 75. (South Africa)

Bardopoulos, A. M., (2015), *eCommerce and the Effects of Technology on Taxation*. Retrived April 9, 2021, Available at: <http://www.springer.com/series/8808>

International Trade Administration, (2020), *South Africa – Country Commercial Guide*. Retrieved April 5, 2020. Available at: <https://www.trade.gov/knowledge-product/south-africa-ecommerce>.

Snail S., 2012, Electronic contracting in South Africa (e-contracts), *Cyberlaw@SA* III pg. 41 – 59

Palmer G., 2014, VAT and e-commerce, South African Institute of Tax Professionals (Garlick & Blousfield Inc), <https://www.thesait.org.za/news/170960/VAT-and-e-Commerce.htm>

Bishop, T. (2020, October 10). *The case against Amazon: Key takeaways from the U.S. House antitrust report on digital markets*. Retrieved April 3, 2021, from GeekWire: <https://www.geekwire.com/2020/analysis-read-antitrust-case-amazon-key-takeaways/>

Brandom, R. (2020, March 3). *The Regulatory Fights Facing Every Major Tech Company*. Retrieved April 5, 2021, from The Verge: <https://www.theverge.com/2020/3/3/21152774/big-tech-regulation-antitrust-ftc-facebook-google-amazon-apple-youtube>

Federal Trade Commission. (n.d.). *About the FTC*. Retrieved April 6, 2021, from Federal Trade Commission: <https://www.ftc.gov/about-ftc/what-we-do>

Jennings, R. (2020, December 28). *China's Regulatory Pressure On Alibaba And Ant Group Sends Tech Stocks Tumbling*. Retrieved April 5, 2021, from Forbes:



<https://www.forbes.com/sites/ralphjennings/2021/12/28/chinas-regulatory-pressure-on-alibaba-and-ant-group-sends-tech-stocks-tumbling/>

National Institute of Metrology, China. (2013). *State Administration for Market Regulation*. Retrieved April 5, 2021, from National Institute of Metrology, China: <https://en.nim.ac.cn/node/647>

Palmer, A. (2020, November 11). *What the EU's investigation of Amazon means for U.S. antitrust probes*. Retrieved April 3, 2021, from CNBC: <https://www.cnbc.com/2020/11/11/eu-investigates-amazon-what-it-means-for-us-antitrust-probes.html>

Zhang, A. H. (2021, February 9). *China is leaning into antitrust regulation to stay competitive with the U.S.* Retrieved April 4, 2021, from Fortune: <https://fortune.com/2021/02/08/china-antitrust-tech-alibaba-tencent-billionaires/>

Badran, M. F., n.d. *Economic Impact of Data Localization in 5 selected African Countries, an imperial study*, Cairo: Cairo University, Faculty of Economics and Political Science.

Mahlobo, M. D., 2012. *THE NATIONAL CYBERSECURITY POLICY FRAMEWORK*, Cape Town: Ministry of State Security.

Presidency, T., 2002. *Electronic Communications and Transactions Act*, Cape Town: Government of South Africa.

Presidency, T., 2013. *Protection of Personal Information Act*, Cape Town: Government of South Africa.

Sutherland, E., 2017. *Governance of Cybersecurity – The Case of South Africa*, Johannesburg: The African Journal of Information and Communication.

Tesfachew, T., 2016. *Data Protection regulations and international data flows: implications for trade and development*, s.l.: Ion Dinca.