T20 INDONESIA 2022 THINK

Policy Brief

CROSS-BORDER DATA FLOW: A TRILEMMA OF MOBILITY, MONETIZATION, AND PRIVACY

Task Force 2

Meaningful Digital Connectivity, Cyber Security, Empowerment

Ibrahim K. Rohman, Indonesia Financial Group Progress
Moinul I. Zaber, United Nations University-Policy Driven on Electronic Governance
Reza Y. Siregar, Indonesia Financial Group Progress
Rizky Rizaldi Ronaldo, Indonesia Financial Group Progress
Mohammad Alvin Prabowosunu, Indonesia Financial Group Progress
Rosi Melati, Indonesia Financial Group Progress

[1] IPAG: The Institute for Policy, Advocacy, and Governance

Abstract

The growing digital economy has been a big boost to economic growth amidst the Covid-19 pandemic. Google, Temasek, and Bain report (2021) projects that the South-East Asia (SEA)'s internet economy will reach $360B by 2025. The e-commerce, food delivery, and digital financial services remain the primary growth drivers in the region. The early adopters have flourished during the pandemic with 60M new users starting to discover the functionality that technology can bring.

The raw material of digital transactions is the data used by both the big-tech and the homegrown-tech companies. Digital transactions are likely to involve cross-border data to streamline the transaction of goods and services, and therefore have a powerful effect on the rise of the digital marketplaces. Data flows across states and nations, and in the process, gets monetized and adds value to the global marketplaces. The use of these data in the exchange of personalized services to the users facilitates the emerging nations to leapfrog the digital progress.

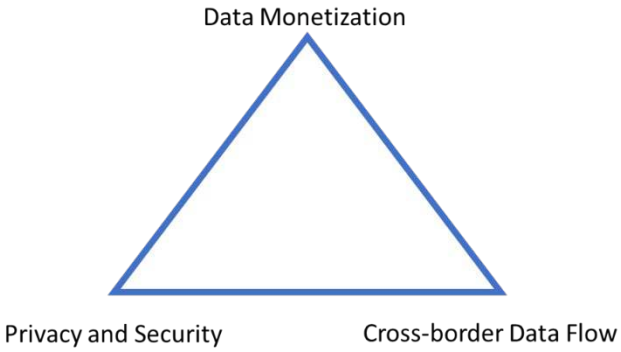
Following the basic principle of the network externalities (Varian, 2010), the value of the digital products grows along with the size of the network. In an increasingly global digital space, only a few rich countries own the digital platforms and provide bulk of the digital services while the rest of the world acts as the service users or secondary innovators. With a balance of computational power tilting on the side of the economic powerhouses, developing countries have little or almost no power over the data being generated by their residents.

Challenges

Free mobility of data is prerequisite for optimizing digitalization

The issue of cross-border data flows around the potential trade-offs between data mobility, personal privacy and security, and the process of data monetization. This trade-off may well be demonstrated by the famous Mundell-Fleming Trilemma of Keynesian Macroeconomics. The Trilemma points out that under a high capital mobility a country cannot simultaneously peg an exchange rate, while maintaining an independent monetary policy and allowing free cross-border financial flows. At best only two of the three targets can be attained. Similarly, we posit that in the case of cross border data flow management, the national regulatory regime cannot uphold personal data privacy and security, while maintaining an independent internal data monetization mechanism and consenting to unchecked cross-border data flow.

Figure 1. Cross-border data flow management



The issue of cross-border data flow is extremely central given data is the lifeblood economic and social interactions (OECD, 2020). Increased digitalization and cross-border transactions have however raised the issue of national and cyber security (Pangestu, M. and H. Lee-Makiyama (2019)). Many have argued that cross-border data should be supported by the privacy and security laws or standards which can be enforced more easily by data localization policy including thru requirements on certain types of data to be stored in local servers, and local processing requirements (OECD, 2020).

Not all countries have the same level of playing field

Figure 2. Data Flow Restriction in ASEAN

Country	Regulation
Indonesia	Economy-wide data localisation (Government Regulation No. 82 regarding the Provision of Electronic System and Transaction, 2012, with implementing acts, 2016); for online services (Electronic Information and Transactions Law, 2008)
Viet Nam	Full data localisation based on both privacy and national security laws (Decree No. 72/2013/ND-CP, Law 24 on Cybersecurity, 2018)
Malaysia	Data flows allowed under certain conditions (Personal Data Protection Act of 2010)
Philippines	Offshoring of financial data forbidden (under Resolution No.2115 of 2015 - Amendments in the Manual of Regulations for Banks and Manual of Regulations for Non-Bank Financial Institutions on the guidelines on outsourcing)
Singapore	Data flows allowed under certain conditions (Public Data Protection Act, 2012)
Thailand	Draft legislation on privacy which would require specific consent by the data subject before an overseas transfer is executed.
Myanmar	No privacy legislation in place, but there are reports of how the government prefers data to be stored locally in some circumstances, and regulators may require on-site inspections.*
Brunei Darussalam	Brunei is alleged to have practices that require data generated within the country to be stored only in servers within the country.**
Lao PDR	The Lao PDR does not have privacy laws or any data flow restrictions.
Cambodia	Cambodia does not have comprehensive privacy laws. Although the right to privacy is a constitutional right, the regulations enforcing this right are in practice very narrow, e.g. the publication of the identity of minors by the press.

Source : *Daniels (2017); **Ezell et al. (2013)

Countries at the early stage of the digital adoption might prioritize the benefits of the internet platforms in the absence of the data regulation and the scrutiny on the data privacy and security. The alignments may be maintained by implementing a regulatory sandbox—a framework set up by a regulator that allows technology companies or start-ups and other innovators to conduct live experiments in a controlled environment under a regulator's supervision. The condition will facilitate the development of the local players—at least in the short run—under the highly protected domestic market.

Nowadays, data privacy and security in some countries already gain close attention from the government. Amongst the ASEAN countries, data localization requirement is already enforced in Brunei Darussalam, Indonesia, Myanmar, the Philippines, and Vietnam through privacy rules or by other means (Pangestu, M. and H. Lee-Makiyama (2019)) – (Figure 2). The implementation of data localization has sparked concerns over its implications on the flow of international data and the fragmentation of the digital world, especially in the digital transaction which could pose damaging economic effects (Bauer et al, 2013). GSMA (2018) argues that the adverse economic effects could potentially cost the GDP growth by more than 50 percent as the spillovers affect trade flows, employment, and investment.

No such thing as free lunch

A country may favor free flow of data and stronger personal security and privacy protection, but it must render the opportunity for internal data monetization. The big tech companies as service providers will benefit from this, but the national smaller techs may face a hard time to comply and to survive the enforced rules of personal security and privacy. The free flow data with weak security and protection may potentially trigger breach of retail data.

In Indonesia, data breaches have occurred several times during the past two years.

1. Health Ministry: data breach of the Indonesia Health Alert Card (eHAC)
2. Healthcare and Social Security Agency (BPJS Kesehatan): data was sold in an online forum known as Raid Forums for the price of 0.15 bitcoins by a user called “Kotz”
3. Cermati and Lazada: data of more than 1 million personal users were illegally sold
4. BRI Life: data of two million life insurance customers were sold online for US$7,000
5. Tokopedia: millions of personal data were stolen from the popular e-commerce site
6. General Elections Commission (KPU): data breach of 2.3 million Indonesians from the General Elections Commission (KPU) website
7. Bank Indonesia: data breach with the leak up to 44GB.

Responding to the case of the data breach, the Indonesian government is drafting a bill of personal data protection (the PDP Bill). The PDP Bill has been designed to become the overarching privacy law in Indonesia. Based on the EU’s General Data Protection Regulation (GDPR), the PDP Bill has made some significant and much-needed changes to data privacy protection and will bring it more in line with standards currently applied by other countries, especially the GDPR (Partner ABNR, 2021).

Proposals for G20

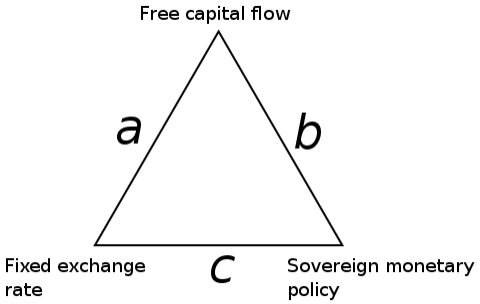
Our Research Note highlights the debate on the Cross-border Trilemma and how countries should adapt their digitalization strategy, in-particular on its data flow. We review the pros and cons, and the role of global cooperation fully supported and driven by the G20 members for countries around the world, particularly the emerging markets, to navigate the Trilemma and achieve the maximum potential benefit in the digitized economy.

1. *Defining the Trilemma of Data Flow*

To better comprehend the Trilemma of Data Flow, we first should understand the basic concept of the Impossible Trilemma and its mechanics. In the world of international economics and finance, the Mundell-Fleming concept has laid out the foundation of the Impossible Trilemma based on their articles from 1961-1963 (Boughton, 2003). The Impossible Trilemma was then popularized by Obstfeld and Taylor (1997), who made the term widely used in the fields of international macroeconomics and finance. The concept of Impossible Trilemma points out that monetary policy makers, in-particular, can't achieve three policy objectives simultaneously: fixed exchange rate, free capital movement, and independent monetary policy. Episodes of early financial crises demonstrate the Impossible Trilemma, including the East Asian financial crisis in 1997-1998 (Patnaik and Shah, 2010). At best only two of the three targets can be attained (Figure 3).

- **Option (a)**: A stable exchange rate and free capital flows, but not an independent monetary policy. Because setting a domestic interest rate that is different from the world interest rate would undermine a stable exchange rate due to appreciation or depreciation pressure on the domestic currency.
- **Option (b)**: An independent monetary policy and free capital flows, at the potential cost of a volatile exchange rate.
- **Option (c)**: A stable exchange rate and independent monetary policy, requiring the use of capital controls (no free capital flows).

Figure 3. The Illustrative Model of Impossible Trilemma

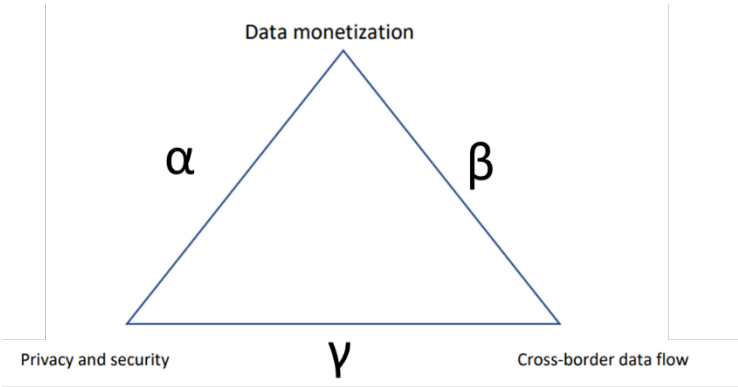


Source: Oxelheim (1990)

The Impossible Trilemma framework and mechanics can also be applied beyond international finance and economics. Albeit lacking mathematical proofs, we can elaborate on how the concept of Impossible Trilemma can be adapted for policy strategies of cross-border data flow. The issue of cross-border data flow revolves around potential trade-offs between data mobility, personal privacy and security, and the process of data monetization. The potential tradeoff mainly came from the debate of how data liberalization is detrimental towards data privacy. Many governments impose regulations to limit, or even completely prohibit data to be stored outside of the jurisdiction due to privacy and other non-economic concerns. On one hand, localized data might, arguably, lead to more trustworthy data security and personal data privacy might be safeguarded relatively easier. But on the other hand, localized data might be detrimental towards trade in services, as data can be monetized and hence beneficial for a country's economic growth. Similarly, we posit that in the case of cross border data flow management, the national regulatory regime cannot uphold personal data privacy and security, while maintaining an independent internal data monetization mechanism and permitting unchecked cross-border data flow (Figure 4).

In summary, it is least likely that a country can achieve all three goals in their digitization and data strategy. If all three goals are pursued, then as demonstrated by the Impossible Trilemma of International Finance, the probability of not achieving at least one of the goals is substantially greater. For instance, overutilized data utilization might trigger data hacking, hence data privacy can be threatened, and partner countries might 'close' the data flow border, rendering data monetization from foreign companies out of equation.

Figure 4. The Illustrative Model of Impossible Trilemma



Source: IFG Progress

Therefore, there are three options that the governments can pursue to achieve two out of three goals of data flow strategy:

- **Option (α)**: Big data monetization potential with secure data privacy, but monetization will only be done locally due to data localization, as cross-border data flows will be limited in this option.
- **Option (β)**: A fairly-open (cross-border) data flow with huge data monetization potential, but with a relatively bigger risk of data privacy and security leaks.
- **Option (γ)**: A relatively high degree of data privacy and security with fairly open (cross-border) data flows, but little-to-none impact on the real economy due to small data monetization opportunities.

These options elaborated above are available for any government, especially from the G20 countries, but there's no one solution that fits all problems. For example, countries at the early stage of the adoption process might prioritize the benefits of the internet platforms in the absence of the data regulation and the scrutiny on the data privacy and security. The alignment may be maintained by implementing a regulatory sandbox- a framework set up by a regulator that allows technology companies or start-ups and other innovators to conduct live experiments in a controlled environment under a regulator's supervision. The condition will help the local players to prosper (at least in the short run) under the highly protected marketplace.

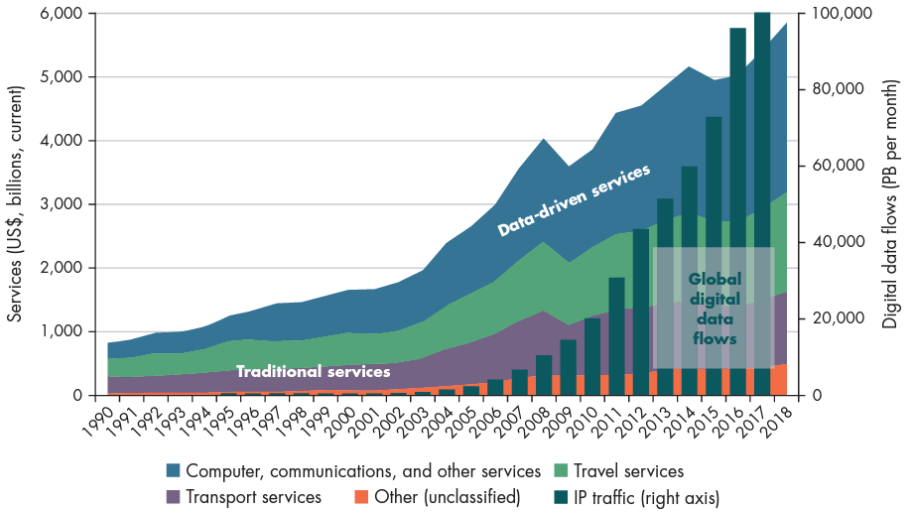
On the other hand, countries with more saturated technology companies' market landscape may favor free flow of data along with stronger personal security and privacy protection, but it must render the opportunity for internal data monetization. The big tech companies as service providers will benefit from this, but the domestic/local smaller techs may face hard time to comply and to survive the enforced rules of personal security and privacy.

2. *Real World Cases of the Data Trilemma in G20 Countries*

Next, we will present selected real-world experiences on the Data-Flow Trilemma. As demonstrated in Figure 5, there appears to be a shift in the regime of the Data Flow policy. Following the crash of the dot-com era in early 2000, global data flows increased exponentially, especially since 2005. Interestingly, the rise in the data flows coincided with the rapid rise in the trade of services trade, implying there is a positive correlation between cross-border data flows and real economy. This trend pointed to the sharp rise in the data monetization.

According to the World Bank Policy Research Working Paper (2021), co-authored by Ferracane & van der Marel, data openness for Indonesia as an emerging economy and a member of the G20 group of countries, remains limited (Figure 6). Indonesia imposes a set of regulations on the data movements, including economy-wide data localization (Government Regulation/ Peraturan Pemerintah (PP) No. 71/2019 regarding Provision of Electronic System and Transaction); for online services (Electronic Information and Transactions Law/ Undang-Undang (UU), 2008). While data localization can be a good policy to attract investments and job creation for the country, it might undermine the progress of Indonesia's integration to the global financial system, and hence narrowing data monetization opportunities.

Figure 5. Global Data Flows and Services Trade

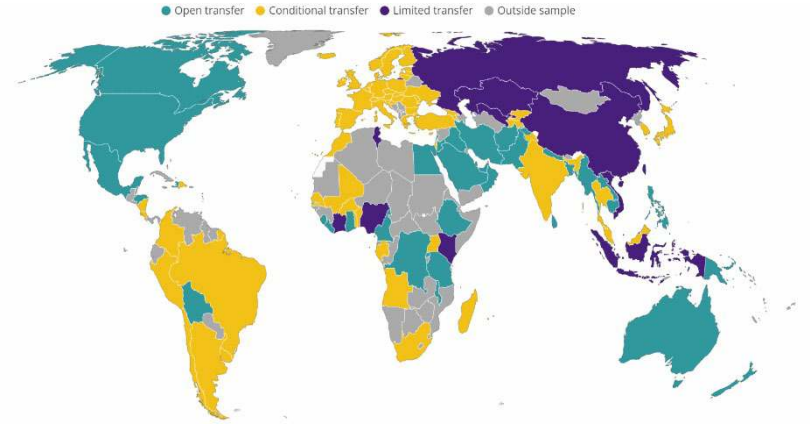


Source: World Bank Development Report (WDR), 2021

Similarly, China also implements strict limitations on transfers of personal and other important data, ranging from financial information and telecommunications to health and medical activities and mapping services, as well as online publishing. Operators are required to store and process certain personal data in China. In addition, foreign companies may have to apply for permission before transferring personal data out of the country. Therefore, it is estimated that

the degree of data monetization is relatively low compared to countries with open cross-border data flow.

Figure 6. Degree of Data-Openness by Country



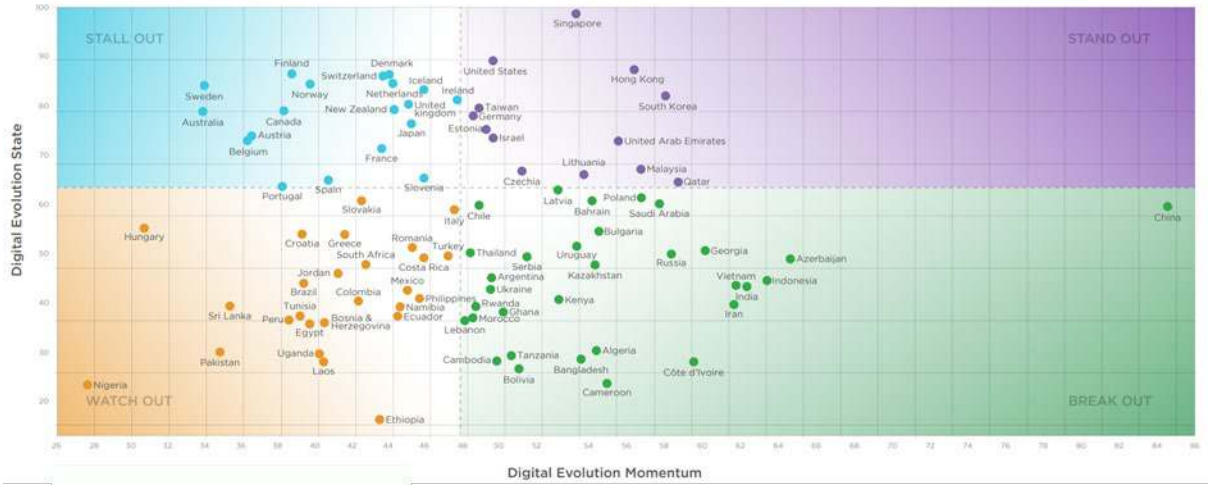
Source: Ferracane, Martina Francesca, and Erik van der Marel, 2021

3. *The Digital Maturity of Economy*

Based on classification of the Fletcher School (2021), the development (maturity) of digital economy can be classified into four stages, 1) Stand-out, 2) Break-out, 3) Stall-out, and 4) Watch-out (Figure 7). The stage of the development or maturity depends on two important indicators: 1) Digital Evolution State, and 2) Digital Evolution Momentum:

1. **Stand-out Economies** (Countries that show digital advancement and exhibit high momentum of digital evolution)
2. **Stall-out Economies** (Countries that show digital advancement and but with slower momentum of digital evolution)
3. **Break-out Economies** (Countries that have low score in digitalization but evolving rapidly)
4. **Watch-out Economies** (Countries that have low score in digitalization and slow momentum of digital evolution)

Figure 7. The Development (Maturity) of Digital Economy



Based on these four classifications, out of 90 countries, 26 of them are classified as Watch-out economies, 32 are classified as Break-out, 19 are Stall-out, and lastly, 13 are Stand-out (Table 1).

Table 1. The Development (Maturity) of Digital Economy Based on Category & Income Group

Category	High income	Upper middle income	Lower middle income	Low income	Total
Stand Out	12	1	0	0	13
Stall Out	19	0	0	0	19
Break Out	6	12	13	1	32
Watch Out	6	11	7	2	26
Total	43	24	20	3	90

Most high-income countries are classified as Stand-out & Stall-out economies, while Upper-middle income, Lower-middle income, & Low-income are classified as Break-out and Watch-out economies. Using these stages as the basis of our analysis, we can map out how the development (maturity) of the digital economy in every country influences the trade-offs described under the Impossible trilemma (Figure 8).

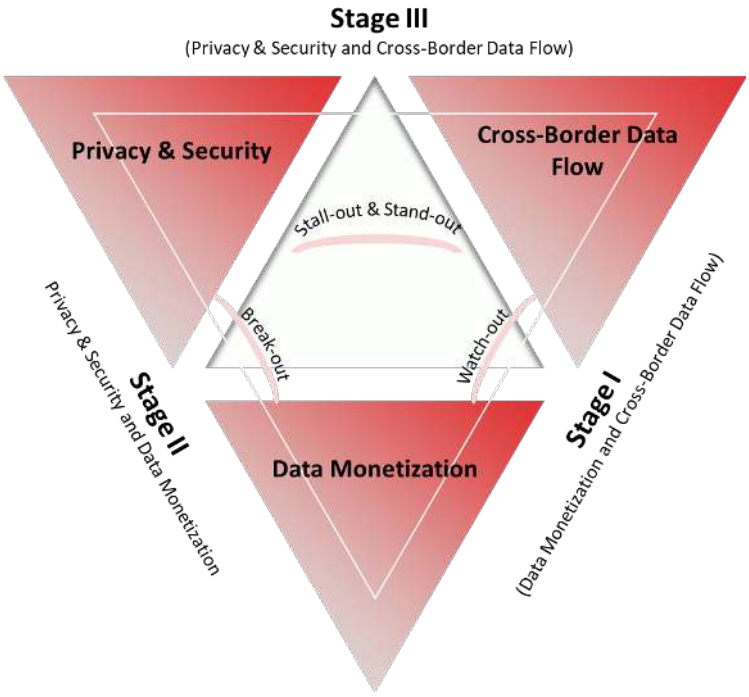
From the framework in Figure 8, we could further classify the economy into three key stages:

a. **Stage 1**: Watch-out economies
b. **Stage 2**: Break-out economies
c. **Stage 3**: Stall-out and Stand-out economies

Watch-out economies are classified into stage I because they are still focusing on data monetization and cross-border data flow as their main objectives. Countries that score

exceptionally low both in evolution state and momentum might prioritize the benefits of the internet platforms in the absence of the data regulation and scrutiny on the data privacy and security.

Figure 8. Impossible Trilemma Staging Based on The Development (Maturity) of Digital Economy



As the digital penetration of the Watch-out economies becomes more mature, they move to the next stage (stage II) where they strengthen their privacy and security without sacrificing data monetization. But achieving those two objectives comes at the cost of lower degree of cross-border data flow. We see this practice in numerous countries are in this group nowadays as data localization has forced and distorted cross-border data flows. The last stage (stage III) or what we call as the digital north, is the stage where countries maintain prudent and safe cross-border data flow while keeping their data privacy and security with a remarkably high standard. Countries that could accomplish this last stage is mainly consist of high-income economies with strong and advance technology company that can comply with this standard. Moving and navigating countries from stage I into stage III is key to maximizing the benefit of a digitized economy. To reach the transition from Stage I to Stage III objectives, we propose four measures for the G20 economies.

1. **Open & Inclusive National Data Strategy**
   Competitiveness and innovation will improve with less data protectionism and more data privacy rights. To fully unlock and realize the potential of the New GDP, economies must promote data flow openness while ensuring proper privacy protections for their inhabitants. Singapore, Japan, Canada, and the Netherlands, which are classified as the Digital North (the northern half of the Digital Evolution grid), are good examples of this approach, with increased openness to data flows and robust privacy protections. China, Russia, Turkey, and Saudi Arabia, all in the Digital South (the southern half of the Digital Evolution grid), score poorly on each of these measures. Data localization laws are becoming increasingly common, posing restrictions to data accessibility that are not only a burden to global growth but also a threat to national security.

2. **Interoperability Strategy**
   To fully maximize the potential of data, a country needs not only to have an open access policy that is easy to be interpreted and understood by other parties. This concept can be adopted by establishing an interoperability strategy. The ability for any sector information systems to flexibly exchange, transform, and interpret shared data across multiple systems and devices to increase productivity & efficiency, to reduce cost, and to reduce errors. With this strategy, data would not only be useful and meaningful for a specific sector, but also for other sectors. Hence, helping not only their core businesses but also opening other opportunities that have not been discovered.

3. **Global Cooperation in Expanding Consumer Choices and Benefits**
   Joint global cooperation, facilitated by the cross-border data flow, is important in unlocking the optimal benefit of a digitized economy as it could extend and broaden both domestic markets as well as businesses. Flexible cross-border data-flow rules would enable developing-country enterprises to benefit not just from providing services to global markets, but also from getting competitive digital services in return. Augmedix, a Bangladeshi company, for example, provides remote help to medical practitioners in the United States. These doctors wear smart glasses that allow their helpers in Bangladesh to attend patient consultations and to release medical prescriptions. This two-way data exchange, as well as the high-value added services provided by Bangladeshi assistants, is only possible because both countries—the US and Bangladesh—allow sensitive and personal data to traverse borders (World Bank, 2021).

4. Keeping Trade Openness thru the Cross-Border Data Flows

According to a 2018 report from the Organization for Economic Cooperation and Development (OECD), digitalization is associated with increased trade openness, which allows companies to sell more products to more markets, and a 10 percent increase in bilateral digital connectivity increases service trade by over 3.1 percent. Businesses can use data to produce value only if data can travel freely across borders. As a result, data localization reduces the potential influence of data-intensive services on economic productivity and innovation. Based on ITIF (2021) countries that implement data-localization, a measure to force and confine data within a country's borders, are increasing very rapidly around the world. The adoption of the data localization and the related data categories included in the policy by more countries is a rising threat to a global digital economy that is open, rule-based, and dynamic.

Conclusion

The issue of cross-border data revolves around potential trade-offs between data mobility, personal privacy and security, and the process of data monetization. The cross-border data flow is a complex phenomenon that entails both the pros and cons. The challenge is compounded further by the balancing between the development of the digital economy and the cost that it entails, especially for the developing nations. This paper becomes relevant as the G20 group comprises many countries with vast differences in the digital technology development stages and landscapes. The major and developed G20 economies are the home/origin of the big-tech firms and those firms (such as the global financial institutions) that will benefit from a greater freedom of cross-border data while achieving high monetization and maintaining data privacy and security. Therefore, the challenges posed by the Trilemma would be highly relevant for the G20 Countries.

References

Bhaskar Chakravorti, Ravi Shankar Chaturvedi, Christina Filipovic, and Griffin Brewer, Digital in The Time of Covid, p. 8

ECIPE (Digital Trade Estimates Project), Restrictions on Cross-Border Data Flows, 15 April 2022, https://ecipe.org/dte/database/?country=FR&chapter=829&subchapter=830.

Nigel Cory And Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them”, in Information Technology & Innovation Foundation, July 2021, p. 1

Organization for Economic Cooperation and Development (OECD), Digital Trade and Market Openness Paris: OECD Trade Policy Papers, No. 217, 2018

World Bank, Data For Better Lives, Washington, 2021, p. 242, https://www.worldbank.org/en/publication/wdr2021