ISTANBUL BILGI UNIVERSITY
INSTITUTE OF GRADUATE PROGRAMS
INFORMATION TECHNOLOGY LAW MASTER'S PROGRAM

LEGAL AND ECONOMIC ANALYSIS OF DATA LOCALISATION PRACTICES FOR FINANCIAL INSTITUTIONS IN TURKEY

Direnç BADA
118691004

Doç. Dr. Leyla KESER BERBER

ISTANBUL
2020

LEGAL AND ECONOMIC ANALYSIS OF DATA LOCALISATION PRACTICES FOR FINANCIAL INSTITUTIONS IN TURKEY

TÜRKİYE'DEKİ FİNANSAL KURULUŞLARA UYGULANAN VERİ LOKALİZASYONU KURALLARININ HUKUKİ VE EKONOMİK ANALİZİ

Direnç BADA
118691004

Tez Danışmanı : **Doç. Dr. Leyla KESER BERBER** (İmza) .....
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : **Dr. Öğr. Üyesi Mehmet Bedii KAYA** (İmza) .....
İstanbul Bilgi Üniversitesi

Dr. Öğr. Üyesi Kadir BAŞ (İmza) .....
Marmara Üniversitesi

Tezin Onaylandığı Tarih : 30.12.2020
Toplam Sayfa Sayısı : 95

Anahtar Kelimeler (Türkçe)
1) Veri Lokalizasyonu
2) Veri Koruması
3) Finansal Kuruluşlar
4) Yurt Dışı Veri Transferi
5) Ekonomik Etki

Anahtar Kelimeler (İngilizce)
1) Data Localization
2) Data Protection
3) Financial Institutions
4) Cross-Border Data Transfers
5) Economic Impact

TABLE OF CONTENTS

SECTION 3
LEGISLATIVE FRAMEWORK AND PRACTICES

ABBREVIATIONS

AI	Artificial Intellegince
AISP	Account Information Service Provider
AML	Anti-Money Laundering
CFT	Combating the Financing of Terrorism
CII	Critical Information Infrastructure
CoE	Council of Europe
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DPA	Data Protection Authority
EU	European Union
FDI	Foreign Direct Investment
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IMF	International Monetary Fund
IoT	Internet of Things
PDPL	Personal Data Protection Law No. 6698
PISP	Payment Initiation Service Provider
PSD2	Payment Service Directive 2
PVA	Process Value Analysis
MLAT	Mutual Legal Assistance Treaties
SaaS	Software as a service
TFP	Total Factor Productivity
TPP	Trans-Pacific Partnership

TPPs	Third-Party Service Providers
UK	United Kingdom
UNCTAD	United Nations Conference on Trade and Development
US	United States
USMCA	United States–Mexico–Canada Agreement

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

This thesis aims to evaluate the legal and economic impact of data localization rules in Turkey on banks, payment providers, and electronic money institutions. Before delving into the topic, in Section 1, relevant reports suggesting the importance of data flows were examined. Also, international agreements were examined with a specific focus on the parts related to financial services, and data localization.

In Section 2, categories of the data localization practices were explained. In Section 3, this categorization was used to evaluate the rules in Turkey, EU, India, China and Russia. For comparative reasons, the discussion is furthered by examining the relevant legal frameworks of the respective countries. It can be observed that China and Turkey are applying the strictest rules for financial institutions among countries examined for the purposes of this thesis. Moreover, the evaluation carried out in this thesis shows that there are inconsistencies and uncertainties which result from the overlapping legislations and designated powers of the relevant competent authorities in Turkey.

Section 4 reviews the economic reports that quantify the effect of data localization rules by using measures such as GDP and TFP. The impact of such rules on the financial industry was also examined by quantifying the additional costs brought with such rules and their effects on innovation, security, open banking, mobile money remittances, and e-commerce. Lastly, PayPal's exit was used as an example to underscore further the effects data localization practices have in Turkey.

As a result of the economic examination, it is evident that all the countries that apply data localization rules are negatively affected, whereas the most affected ones are the countries and sectors that are data-intensive. The financial industry is among the most affected sectors since it is highly dependent on data flows, and the localization rules increase IT expenditures, limit the use of new technologies, and create a security vulnerability.

Keywords: Data Localization, Data Protection, Financial Institutions, Cross-Border Data Transfers, Economic Impact

ÖZET

Bu tez ile Türkiye'de banka, ödeme ve elektronik para kuruluşları için yürürlükte olan veri lokalizasyonu kuralları incelenerek, bu kuralların ekonomik ve hukuki değerlendirmesi yapılmıştır. Birinci Bölümde, verinin ekonomi için önemini ortaya koyan raporlar, uluslararası sözleşmeler ve tek ve çok taraflı ticaret anlaşmalarının finans kuruluşlarını ilgilendiren kısımları özellikle veri transferi ve lokalizasyonu açısından incelenmiştir.

İkinci Bölümde veri lokalizasyonu uygulamalarının kategorizasyonuna yer verilmiştir. Üçüncü Bölümde bu kategorizasyon kullanılarak, Türkiye, Hindistan, Avrupa Birliği, Rusya ve Çin'deki mevzuatlar karşılaştırmalı bir şekilde incelenmiş, incelemeye konu ülkeler arasında Türkiye ve Çin'in en katı kurallara sahip ülkeler arasında olduğu tespit edilmiştir. Ayrıca Türkiye'de yetkili kurumların yetkilerinde ve finansal kuruluşlara uygulanan mevzuatların veri yönetimiyle ilgili kısımlarında çakışmalar olduğu tespit edilmiştir.

Dördüncü Bölümde veri lokalizasyonu kurallarının ekonomiye etkisini, Gayri Safi Milli Hasılası ve Toplam Verimlilik Faktörü gibi kavramlar ışığında ortaya koyan raporlar incelenmiştir. Bunların yanı sıra, veri lokalizasyon kurallarının finansal kuruluşlara getirdiği ek maliyetler ile birlikte inovasyon, güvenlik, açık bankacılık, para transferi ve e-ticarete olan etkisi de incelenmiştir. Son olarak Türkiye'deki veri lokalizasyonu kurallarının bir sonucu olarak piyasadan çıkış yapan PayPal'in durumu örnek vaka olarak ele alınmıştır.

Ekonomik analiz sonucunda, veri yoğunluğu yüksek ülke ve sektörlerin diğerlerine göre daha fazla etkinlendiği sonucuna varılmıştır. Finans sektörünün veri yoğunluğu yüksek sektörler arasında olduğu ve lokalizasyon kurallarının işlem maliyetlerini artıracağı, yeni teknolojilerden istenen düzeyde yararlanmasının önüne geçeceği ve güvenlik açısından zafiyetler yaratacağı değerlendirmesine yer verilmiştir.

Anahtar Kelimeler: Veri Lokalizasyonu, Veri Koruması, Finansal Kuruluşlar, Yurt Dışı Veri Transferi, Ekonomik Etki

INTRODUCTION

The digitization of the economy increased the significance of cross-border data flows. The cross border data flows contributes more to the world economy than the trade of traditional goods[1]. Despite the increasing importance of cross-border flows, various policies restricting data transfers were enacted for various reasons, such as personal data protection, economic security, and sovereignty.

Europe prohibits its members from putting barriers to each other for cross-border data transfers and adopts the principle of free flow of data within the European Economic Area territory. Their rules also go beyond the EU borders and influence all entities outside Europe that targets consumers in Europe. They have also initiated international agreements such as Convention 108 and Convention 108+ to set a unified practice for personal data rules. Countries also started to include data localization ban in trade agreements such as TPP and CPTPP.

Meanwhile, with its vast population, China created an ecosystem led by local players covered by a vast firewall. The strategy successfully created huge companies, such as Alibaba (AliPay) and Tencent (WeChat Pay). However, their decisions to prevent cross border data flows, requiring local installation and favoring national companies started to backlash, resulting in the ban of Chinese companies worldwide[2][3]. Despite the recent challenges, Chinese success encouraged some countries to devise strict data governance rules.

Data is fuelling new technologies such as AI, IoT, and blockchain. These technologies can significantly improve our lives by transforming almost all the

[1] Mckinsey Global Institute, 'Digital Globalization: The New Era of Global Flows' (2016) 11 <https://www.mckinsey.com/~/media/McKinsey/Business Functions/McKinsey Digital/Our Insights/Digital globalization The new era of global flows/MGI-Digital-globalization-Full-report.ashx>.
[2] Maanvi Singh, 'Trump Bans US Transactions with Chinese-Owned TikTok and WeChat' *Guardian* (2020) <https://www.theguardian.com/technology/2020/aug/06/us-senate-tiktok-ban>.
[3] Stephanie Findlay, 'India Bans Dozens of Chinese Mobile Apps' *Financial Times* (2020) <https://www.ft.com/content/08e15c26-48e0-4540-a040-1a8782e84f2e>.

sectors, while they can be used to expose the vulnerable and manipulate the system[4]. The financial sector is one of the most data-driven sectors and has a substantial role in the world economy. As the most traditional financial institutions, banks are taking steps to implement the new technologies, whereas the fintech companies challenge their dominance with various business models and technologies. The monetary system is also challenged by the rise of cryptocurrencies and by the technology behind it.

The data practice of financial institutions is changing according to the latest technologies, and the regulators are trying to balance the interest of the consumer, company, and country. Many countries introduced restrictions to cross-border transfer of financial data due to their sensitivity. Financial data is the most restricted data worldwide. However, it is arguable if localizing data and preventing data flow outside the country is to provide the required safeguard, protect the citizens, and foster the economies.

Although it is also important to note that there are considerable efforts observed in the legal framework towards modernizing the financial industry[5], Turkey is among the countries that apply strict localization rules for banks, payment services, and electronic money institutions.

Methodology

This study is based on the doctrinal method incorporating comparative and interdisciplinary methods. Legislative frameworks of Turkey, Europe, Russia, China, and India were examined and compared. Additionally, economic reports

[4] Guardian, 'The Cambridge Analytica Files' *Guardian* (2018) <https://www.theguardian.com/news/series/cambridge-analytica-files>.

[5] See for example The Central Bank of the Republic of Turkey, Regulation on the Generation and Use of the Turkish QR Code in Payment Services 2020.; Banking Regulation and Supervision Agency, Regulation on Banks' Information Technology and Electronic Banking Services 2020.; Banking Regulation and Supervision Agency, Draft Communiqué on Remote Identification Methods to be used by Banks 2020.

regarding the impacts of localization rules were also delved into providing a broad picture emerging as a result of practices of such localization rules. During the study, unstructured interviews with numerous experts were conducted and inserted into this thesis under anonymity principles.

Scope and Objective

The evaluation provided in this dissertation is inclined to focus on the economic and legal aspects of data localization practices implemented on financial institutions in Turkey and aims to answer the following questions:

1 – What is the importance of cross-border data flows?

2 - How do Turkey, EU, India, China, and Russia handle data?

3 – Are special rules applied for financial institutions in respect of data practices? If so, what are they, and how are they implemented?

4 – Overall, where is Turkey positioned? What are the rules, practices, and outcomes of such rules?

5 – What is the effect of data localization rules on the economy and financial industry?

In order to answer these questions, Section 1 emphasizes the importance of data to the world economy by reviewing the recent reports, the international agreements, and bilateral and multilateral trade agreements. Section 2 examines the restrictions on cross-border data flows and categorizes the restriction regimes. Section 3 examines the provisions related to processing, transferring, and storing data in Turkey, the EU, India, China, and Russia and compares their practice. Section 4 aims to analyze the effect of the localization rules on the economy and the financial sector.

SECTION 1
DATA-DRIVEN ECONOMY

1.1. OVERVIEW

Global data flows are growing every day, thanks to digitalization, increasing internet usage and technological developments. According to Mckinsey's study, $2.8 trillion (out of $7.8 trillion) was added to the global GDP in 2014 as a result of data flows. The report indicates that cross-border data flows generate more economic value than the trade of products, and the globalization structure is changing accordingly.[6] The growth will continue. According to the International Data Corporation Report ("IDC report"), "the global data sphere will grow from 33 zettabytes in 2018 to 175 zettabytes in 2023."[7]

The growth in the global data sphere and the upcoming technologies will also change how we store and process data. According to the IDC report, approximately 80% of data processing occurs in data centers and centralized computing facilities today and 20% in smart connected objects, such as cars, home appliances or manufacturing robots, and computing facilities close to the user. By 2025 these proportions are likely to be the opposite[8] , and the machines will continuously exchange data with each other. The calculation clearly shows that IoT technologies' influence will be inevitable, thus shifting to the cloud from traditional data centers. Accordingly, IDC predicts that in 2025, 49% of the world's stored data will be in public cloud centers.[9]

[6] Mckinsey Global Institute (n 1) 11.
[7] David Reinsel, John Gantz and John Rydning, 'The Digitization of the World - From Edge to Core' (2018) 3 <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>.
[8] European Commission, 'A European Strategy for Data' (2020) 2 <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf>."
[9] Reinsel, Gantz and Rydning (n 7) 4.

The previous trade agreements were solely focusing on the trade of products or conventional services. Due to its importance, the trade agreements started to contain rules ensuring the free flow of data. The countries are rushing to form and enter bilateral trade agreements and multilateral trade agreements to secure their economic interests.

Europe prohibited to put barriers on the cross border data flows among its member-states by emphasizing its importance to their economy. The CoE member states initiated Convention 108 and 108+ and extended the data protection rules to non-member states to form a unified practice. The signatory countries of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) prohibits any rules restricting the cross-border data flow with some exceptions, such as data protection regulations. US sees data localization as one of the main threats towards their tech companies and defend full liberalization. China aims to create a domestic data ecosystem led by Chinese companies. India is applying a hybrid approach and aims to secure the domestic players' interest by being sensitive to international companies' needs. Data is shaping the new world order, just as oil did a century ago.

1.2. INTERNATIONAL AGREEMENTS

1.2.1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[10]

Convention 108 is the first legally binding international agreement in the data protection field and was signed in 1981 by the members of the Council of Europe

[10] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.

(CoE). Nine non-member states implemented the agreement, and 55 countries ratified it[11]. Turkey is among the countries that signed and ratified the Convention.

The main aim of Convention 108 is to protect the right to the respect of privacy and ensure the freedom of information regardless of frontiers. According to Article 5, the processing of personal data must be carried out fairly and lawfully[12]. Some provisions define how data must be kept and used. Article 6 specifies special categories of personal data and indicates that the special categories of personal data might not be processed unless national laws provide appropriate safeguards[13].

Article 12 regulates the cross border data transfers and prohibits any restriction for the sole purpose of the protection of privacy. There are only two exceptions; (i) specific regulations for certain categories of data (ii) to avoid transfers to non-member through the member states by circumventing the legislation.

"Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (Treaty No.108)"[14] signed in 2011, set forth new rules for cross-border transfers to non-member states. Accordingly, the cross-border transfers of personal data to non-signatory states may only be held in the recipient country or organization that provides an adequate protection level. The exemptions are (i) provided by the domestic law for the interest of data subject or important public interest and (ii) the safeguards provided by the controller and approved by the competent authority.

[11] Council of Europe, 'Chart of Signatures and Ratifications of Treaty 108' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=w4NkUCsR> accessed 18 September 2020.
[12] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (n 10) Article 5.
[13] ibid Article 6.
[14] Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (Treaty No.108) 2001.

The explanatory report states that the free flow of personal data is a key principle of the agreement, and the controls introduced by nations must not prejudice this principle[15].

1.2.2. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+)[16]

CoE decided to modernize the Convention 108 in line with technological developments by keeping the main structure. Convention 108+ is signed by 42 countries and ratified by 9 of them[17]. Turkey is among the few CoE members that did not sign the agreement. However, the Turkish DPA states that they plan to sign Convention 108+.

Convention 108+ contains similar provisions with the General Data Protection Regulation (GDPR). Article 5 and Article 6 regulates the data processing of personal data and special category of personal data, respectively.

Article 14 of Convention 108+ regulates the transborder flows of personal data. Accordingly, the parties undertake not to prohibit or subject to special authorization the cross-border transfer of personal data among member states for the sole purpose of personal data protection. There are two exemptions (i) to avoid transfers to non-member states through the member states by circumventing the legislation (ii) if the member state is bound by harmonized rules of a regional international organization[18]. According to the explanatory report of Article 14, it is stated that the exemptions must be interpreted restrictively, and parties cannot rely on it in

[15] Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 3."
[16] Convention for the protection of individuals with regard to the processing of personal data (Convention 108+) 2018.
[17] Council of Europe, 'Chart of Signatures and Ratifications of Treaty 223' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures> accessed 23 September 2020.
[18] Convention for the protection of individuals with regard to the processing of personal data (Convention 108+) Article 14/1.

cases where the risk is minor. The second exemptions refer to regulations such as the GDPR. GDPR recognizes the implementation of Convention 108 as an important factor when assessing the third countries adequacy application.

Convention 108+ also regulates personal data transfers to non-party states. Accordingly, the transfer of personal data may only take place to a non-party state if an appropriate level of protection based on the provisions of this Convention is secured[19]. The appropriate level of protection could be secured by: "(i) ad hoc or approved standardized safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer, or (ii) the law of that State or international organization, including the applicable international treaties or agreements."[20]

Nevertheless, the cross border transfer could be held even if the appropriate level of protection is not maintained in the following circumstances; (i) the explicit consent of the data subject, (ii) the specific interest of the data subject, (iii) public interest (iv) required for freedom of expression (v).[21] Article 14 aims to enable cross border personal data transfers to non-parties by ensuring the protection of individuals.

1.2.3. Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

The Trans-Pacific Partnership (TPP) was a trade agreement signed by 12 countries, including the United States on 4 February 2016. President Donald Trump withdrew the US signature from TPP in 2017; thus, it did not enter into force. The remaining countries negotiated a new trade agreement called the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), which incorporates

[19] ibid Article 14/2.
[20] ibid Article 14/3.
[21] ibid Article 14/4.

most of the provisions of the TPP. The CPTPP countries represents a combined population of nearly 500 million people and more than 13% of global trade.

The CPTPP acknowledges the free flow of data across borders for service suppliers and investors as part of their business activities. The signatory countries have retained the ability to maintain and amend regulations related to data flows with data protection regulations in a way that does not create trade barriers[22].

Chapter 14 covers Electronic Commerce. Article 14.11[23] of TPP indicates that the "parties shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person."[24] The only exemption is for public policy means and provided that the measure: "(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective."

One of the key outcomes of CPTPP is that the member countries have committed not to impose localization requirements that would force businesses to build data storage centers or use local computing facilities, providing certainty to businesses considering their investment choice[25].

Article 14.13[26] of TPP bans data localization requirements. Accordingly, the parties shall not require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. The only exemptions are for public policy means and provided that the measure: "(a) is not

[22] Australian Government Department of Foreign Affairs, 'CPTPP Outcomes: Trade in the Digital Age' <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/outcomes-documents/Pages/cptpp-digital>.
[23] 'Trans-Pacific Partnership Agreement' (2016) Article 14.11 <https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/tpp-text-and-associated-documents>.
[24] covered person means: (a) a covered investment as defined in Article 9.1 (Definitions); (b) an investor of a Party as defined in Article 9.1 (Definitions), but does not include an investor in a financial institution; or (c) a service supplier of a Party as defined in Article 10.1 (Definitions), but does not include a "financial institution" or a "cross-border financial service supplier of a Party
[25] Australian Government Department of Foreign Affairs (n 22).
[26] 'Trans-Pacific Partnership Agreement' (n 23) Article 14.13.

applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective."

The definition of "covered person" excludes financial institutions and services. Chapter 11 regulates the financial institutions and services. Banking and other financial activities (excluding insurance) were defined widely and covers the following activities: "provision and transfer of financial information, and financial data processing and related software by suppliers of other financial services."

Article 11.6 indicates that each Party shall permit, under terms and conditions that accord national treatment, cross-border financial service suppliers of another Party to supply the financial services specified in the definition. Accordingly, the parties have committed to permit financial institutions to transfer data according to personal data protection regulations.[27]

Unlike the electronic commerce section, the financial service chapter does not include a ban on data localization. The US business community identified the lack of data localization ban for financial services as one of the main issues to be resolved and suggested a prohibition on data localization requirements when financial regulators can access information stored abroad. Despite arguments from the business community to prohibit localization requirements, the US Treasury Department, with the Federal Reserve and the Federal Securities and Exchange Commission, supported the current language to maintain a policy space for US regulators for the possibility to implement such restrictions in the future, citing instances during the 2008-2009 financial crisis when US regulators could not get the needed data[28].

[27] Australian Government Department of Foreign Affairs, 'TPP Outcomes: Financial Services' <https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/outcomes-financial-services> accessed 5 October 2020.
[28] Rachel F Fefer, 'TPP Financial Services Data Flows' <https://fas.org/sgp/crs/row/IN10498.pdf>.

Recently, UK also signed a free trade agreement with Japan. UK sees the agreement as an important step towards joining the CPTPP. One of the important provisions is that the countries agreed to introduce a ban on data localization and improve market access for financial services. According to the UK, this will help UK fintech firms, like Revolut and Transferwise, grow in Japan.[29] China also announced that they plan to join the CPTPP[30].

1.2.4. United States–Mexico–Canada Agreement (USMCA)[31]

United States, Mexico, and Canada reached an agreement to replace the North American Free Trade Agreement (NAFTA) in 2018, and the countries ratified it through their legislators. The trade agreement covers many sectors, including the financial industry.

Chapter 17 of the USMCA contains provisions concerning financial services. Banking and other financial service activities (excluding insurance) were defined widely and contain the following activities besides many other: "transfer of financial information, financial data processing and related software by suppliers of other financial services."

Covered person was defined as; "(a) a financial institution of another Party; or (b) a cross-border financial service supplier of another Party that is subject to regulation, supervision, and licensing, authorization, or registration by a financial regulatory authority of the Party"

[29] UK Government, 'UK and Japan Agree Historic Free Trade Agreement' (*2020*) <https://www.gov.uk/government/news/uk-and-japan-agree-historic-free-trade-agreement> accessed 24 September 2020.
[30] TSUKASA HADANO and TAKASHI NAKANO, 'Xi Says China Will Consider Joining TPP' (*Nikkei Asia*, 2020) <https://asia.nikkei.com/Politics/International-relations/Xi-says-China-will-consider-joining-TPP> accessed 21 November 2020.
[31] 'Agreement between the United States of America, the United Mexican States, and Canada 12/13/19 Text' (2018) <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>.

Article 17.7 regulates the free flow of data[32]. Accordingly, the parties shall not prevent a covered person from transferring information, including personal information, when this activity is for business conduct. The parties also recognize the right to maintain the protection of the personal data and forbids to use such measures to circumvent Article 17.7.

Article 17.8 bans data localization and ensures full access[33]. Accordingly, paragraph 1 recognizes the immediate, direct, complete, and ongoing access by the financial regulatory bodies and bans any potential limitation on the access. Paragraph 2 forbids the parties from obliging a covered person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory if there is full access to the data by the financial regulatory bodies. Paragraph 4 repeats the right for the countries to introduce data protection rules provided that they are not used to circumvent the obligations of this Article 17.8.

To conclude, the agreement provides the free flow of data, bans data localization, and provides full access to the data. The agreement also recognizes the right of the parties to issue data protection measures unless they are not used to circumvent the obligations.

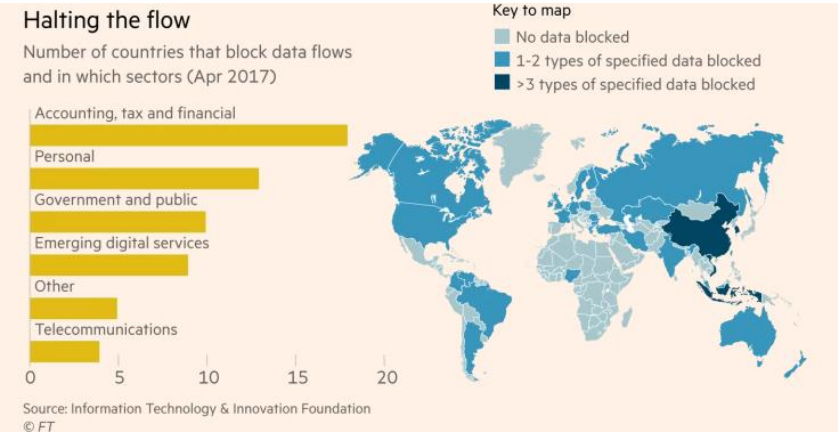
[32] ibid Article 17.7.
[33] ibid Article 17.8.

SECTION 2
CROSS BORDER DATA FLOW RESTRICTIONS

2.1. DATA LOCALIZATION

Many countries implement cross-border data flow restrictions and adopt data localization rules for various reasons, such as privacy, security, public order, sovereignty, and economic security. According to the study of The European Centre for International Political Economy, large economies enforced 84 data localization measures in 2016, which was 31 a decade earlier[34]. Information Technology & Innovation Foundation determined that most of the countries blocked the flow of a specific type of data, and the most restricted ones are accounting, tax, and financial, with 18 countries introducing localization laws [35].

Figure 2. 1 Map of Data Localization Restrictions



Source: Information Technology & Innovation Foundation

[34] Alan Beattie, 'Data Protectionism: The Growing Menace to Global Business' *Financial Times* (2018) <https://www.ft.com/content/6f0f41e4-47de-11e8-8ee8-cae73aab7ccb>.
[35] Niger Cory, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?' (2017) <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>.

2.1.1. Data Localization Regimes

Data localization requirements are broadly defined as "any laws, standards, or policies that require an entity to store data on servers that are physically installed in a specific territory."[36]

The restrictions on cross-border data flows can be categorized into two regimes; strict and conditional. Local storage, local processing, and the ban on data transfer, all separately or together, can be evaluated as "strict," while the conditions that apply to the controller, processor, or recipient country for the transfer would be within the conditional regime[37]. In the conditional regimes, fulfilling the requirements applied to the relevant Party may result in the free flow of data, while if they are not satisfied, that may result in the ban on the data transfer.

2.1.1.1. Strict Regimes

2.1.1.1.1. Local Storage

As part of the local storage requirements, a copy of the data must be stored within the country, and then the data can be transferred abroad. Thus, as long as a copy of the data is saved locally, storage and processing activities can occur outside the country.

[36] World Economic Forum, 'A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy' (2020) 12.
[37] Martina Ferracane, 'Restrictions on Cross-Border Data Flows: A Taxonomy' [2018] SSRN Electronic Journal 1.

2.1.1.1.2. Local Processing

The companies subjected to local processing requirements need to use data centers installed in the country for their processing activities. Thus, the company must either install a data center within the country or to use the data centers of a local provider. The company can also decide to leave the market, as seen with the exit of PayPal from Turkey. Generally, under the local processing requirements, a copy of the data can be sent abroad unless the data is processed locally.

2.1.1.1.3. Ban on Data Transfer

According to this last and most strict regime, data has to be stored, processed, and accessed within the borders of the country. Unlike the local processing regime, the company is not allowed to send a copy of its data abroad to third parties or its subsidiary. Such rules are usually applied to specific industries or sets of data.

2.1.1.2. Conditional Regimes

When a conditional flow regime is in place, the transfer of the data outside of the country is allowed only if the requirements are satisfied. EU's General Data Protection Regulation (GDPR) is an example of conditional regimes. The conditions can apply to both the receiver country and the company together or separately. The conditions set forth with GDPR and other legislation will be examined in section 3.

2.1.1.3. Analysis

The countries can select different approaches for various sectors and data sets. For example, Turkey adopts a conditional regime for personal data, while payment

services, electronic money institutions, and banks are subjected to local processing requirements. While the categorization given above mostly reflects the countries' current practice, there are situations that it does not clearly reflect the data practice of the countries and industries. For example, as explained in the India section, a country can let a company process the data abroad while requiring them only to store the information within the country.

SECTION 3
LEGISLATIVE FRAMEWORK AND PRACTICES

This section will analyze the legal framework applied to the financial industry, mainly banks, payment services, and electronic money institutions, regarding data processing, cross border transfer, and storage. The regulations applied to financial institutions in the EU will be examined, and it will be compared with the situation in Turkey. The practices of Russia, China, and India will also be briefly examined.

3.1. TURKEY

According to Article 20/3 of the Turkish Constitution, the citizens have the right to request their personal data protection. The citizens also have the right to request the correction, deletion and to learn if the data was used for the stated purposes. Personal data can only be processed in cases stipulated by law or with the data subject's explicit consent. The principles and procedures for personal data protection are regulated under Personal Data Protection Law No. 6698 (PDPL), applicable since 2016.

According to the provisions at PDPL, Turkey is among the countries that implement a conditional regime for cross-border data transfers and does not require the entities to keep the data inside the country unless the conditions are met. However, Turkey effectively performs a strict local processing regime to banks, payment services, and electronic money institutions with different regulations.

This section will review the key regulations and decisions concerning the banks, electronic money institutions, and payment services in Turkey.

3.1.1. Personal Data Protection Law No. 6698 ("PDPL")[38] and decisions/guidelines of Data Protection Authority ("DPA")

PDPL was accepted by The Grand National Assembly of Turkey in 2016 and was published in the official gazette the same year. PDPL was prepared according to Article 20 of the Turkish Constitution and has very similar provisions of the Data Protection Directive 95/46 of Europe. The scope of the law is restricted to personal data and does not apply to non-personal data. PDPL concerns all matters where personal data is involved.

Personal data is defined as "all the information relating to an identified or identifiable natural person[39]." Article 5 regulates the conditions to process personal data.

3.1.1.1. Processing Personal Data and Special Category of Personal Data

Personal data cannot be processed unless the explicit consent of the data subject is obtained. There are exceptions where explicit consent is not required for processing. These are: (a) provided by the law, (b) protection of life and physical integrity, (c) execution of a contract, (d) publicly announced, (e) exercise of any right, and (f) legitimate interest of the controller.

Article 6 regulates the conditions to process the special category of personal data, which consists of "*…race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data…*"

[38] 'Law on The Protection of Personal Data No. 6698' <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>.
[39] ibid Article 3/d.

The special category of personal data cannot be processed unless the data subject's explicit consent is obtained. The regulators separate sexual and health data from others. Accordingly, the special category of personal data, excluding sexual and health data, can be processed without the data subject's explicit consent if relevant laws require so. Sexual and health data can only be processed without explicit consent for the protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of healthcare services, and their financing by authorized entities or persons.

3.1.1.2. Cross Border Transfer

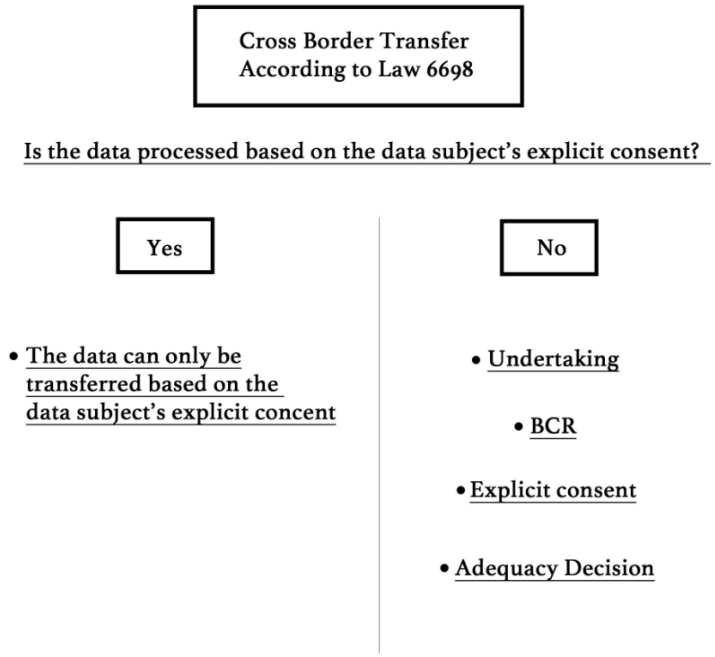
Article 9 regulates the terms of transferring data abroad. Accordingly, the data subject's explicit consent is the main requirement for transferring data overseas, and the only way if the data is processed with the data subject's explicit consent. There are three more ways to transfer data abroad if the data is not processed based on explicit consent;

- **Safe Country List (Adequacy Decision):** The DPA did not announce a safe country list yet. Thus, it is not possible to rely on such a list for cross-border data transfers. While there is no timeline for a list to be announced, in the future, the companies may send data to the selected countries without restrictions.
- **Undertaking approved by DPA:** Many companies filed an undertaking to able to transfer data abroad; however, the DPA did not grant a decision yet. DPA recently announced a guideline highlighting the requirements that the entities must comply with their applications[40], signaling that decisions may come soon.

[40] Turkish Data Protection Authority, Announcement of DPA on the important points that must be evaluated when preparing the undertakings for transferring data abroad.

- **Binding Corporate Rules ("BCR")[41]:** The DPA determined BCR as a new tool to be used for the data transfers based on Article 9/2[42]. The multinational corporations mainly use the BCR due to their global structure, and it may be a useful tool for them in Turkey.

Figure 3. 1 Cross border transfer structure of Turkish Personal Data Law



Source: PDPL

The DPA announced its first decision regarding the violation of the cross-border data transfers and fined Amazon Turkey. Although the DPA recognized that Amazon Turkey filed an undertaking for transferring data abroad, it stated that the only way to transfer data abroad is by obtaining the explicit consent of the data subject since the other methods are not applicable yet.[43]

41 Binding Corporate Rules" is used as a method in the cross-border data transfers to be made between multinational corporate companies.
[42] Turkish Data Protection Authority, 'Announcement of DPA on Binding Corporate Rules' <https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU> accessed 9 May 2020.
[43] Turkish Data Protection Authority, 'Decision of DPA Dated 27 February 2020 and No. 2020/173 Regarding Amazon Turkey' <https://kvkk.gov.tr/Icerik/6739/2020-173> accessed 9 May 2020.

The DPA granted a second decision and fined an automobile company for transferring data to Germany. The automobile company claimed that they have carried out the transfer according to Convention 108, and since Germany is a part of the agreement, they have no restriction on transferring the data. The DPA stated that Convention 108 is not a directly applicable agreement, PDPL must have been taken into account while carrying out the cross border transfer, fined the company, and ordered the deletion of the data held abroad[44].

However, there is a strong opinion from academia and practice claiming that the cross border transfers to the parties of Convention 108 must be held according to the Convention. The grounding of the opinion is that according to Article 90/5 of the Turkish Constitution it is stated that in the case of a conflict between international agreements and laws, which may arise because they contain different provisions on the same matter, international agreements shall prevail, thus, concerning conflicts between the Convention 108 and PDPL, which is part of a persons' fundamental rights and freedoms, Convention 108 must be taken into consideration. Besides, they also state that there has been no action taken by Turkey for any restriction or subject to special authorization by relying on the exceptions outlined in subparagraphs (a) and (b) of Article 12/3 (which adapts the free transfer principles) of the Convention 108.

Despite the tools indicated at PDPL for overseas transfer, considering the practices of the DPA and the implementation of PDPL, we can conclude that the only way to transfer data abroad, whether the data is processed based on the data subject's explicit consent or not, is by obtaining the explicit consent of the data subject for the cross border transfer.

Article 9/6 recognized that other laws must also be evaluated before transferring data abroad. Thus, we will assess the legal framework related to the financial industry.

[44] Turkish Data Protection Authority, 'Summary of the Decision of the Personal Data Protection Board Dated 22/07/2020 and Numbered 2020/559 Regarding "the Transfer of Personal Data Abroad on the Basis of Convention No. 108"' <https://kvkk.gov.tr/Icerik/6812/2020-559>.

3.1.2. Payment and Security Settlement Systems, Payment Services, and Electronic Money Institutions Law no. 6493 (Payment Law)[45] and Secondary Regulations

3.1.2.1. Data Retention and Local Processing

Payment Law is directly applicable to electronic money institutions and payments services. Article 23/1 of Payment Law indicates that the system operator, payment, and electronic money institutions must keep all their documents and records domestically in an accessible and secure manner for at least ten years. The same article also requires the system operator, payment, and electronic money institutions to install their information systems and their backups used for conducting their activities within the country.

Banking Regulation and Supervision Agency (BRSA)[46] issued *Regulation on the Management and Auditing of the Information Systems Used By the Payment and Electronic Money Institutions*[47] ("*Regulation on Information System"*) in line with Payment Law. Article 16 obliges the entities to keep their primary and secondary systems domestically and requires external service providers to keep all their information systems and backups inside the country.

The same Regulation defines primary and secondary systems. Accordingly, primary systems refer to all kinds of software, hardware, infrastructure, and data that help the business to operate, and all kinds of systems that the information relevant to Payment Law are stored securely, electronically, and in an accessible manner. Secondary systems are defined as the backups of primary systems to access all kinds

[45] Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions No. 6493.
[46] With the Amendment Law No. 7192 accepted on 12 November 2019, and effective on January 1, 2020, the duties of BRSA have been assigned to the Central Bank of the Republic of Turkey
[47] Regulation on the Management and Auditing of the Information Systems Used By the Payment and Electronic Money Institutions 2014 1.

of information relevant to Payment Law, and the systems to replace primary systems in case an interruption happens.

3.1.2.2. Sanctions

According to Article 31 of Payment Law, the ones who violate the requirements stated in Article 23 will be sentenced from one to three years of imprisonment, and a judicial fine will be imposed between five hundred days to one thousand five hundred days. Thus, those who do not install their information systems and back-ups inside the country and do not keep all their documents and records domestically in an accessible and secure manner for at least ten years might be punished accordingly. The prosecution and trial could only be initiated if the Central Bank of Turkey submits a written application to the Prosecutors' Office[48]. Besides, the payment services or electronic money institution's license could be canceled if Article 23 is violated[49].

3.1.3. Banking Law No. 5411 and Secondary Regulations

The Banking Law is the primary regulation that sets the rules for banks. A secondary regulation was introduced by BRSA named "Regulation on Banks' Information Technology and Electronic Banking Services (Banking IT Regulation)," which contains important provisions regarding data privacy rules for banks. BRSA is the main regulatory body of banks related to banking activities and is authorized to implement the law, issue secondary legislation, and impose restrictions when found necessary. DPA is also entitled to intervene in matters related to data privacy.

[48] The Grand National Assembly of Turkey Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions No. 6493 (n 45) Article 37.
[49] ibid Article 16/d.

The banks in Turkey are obliged to keep their information systems within the country, similar to system operators, payment, and electronic money institutions, and there are rules in place restricting data transfer abroad.

3.1.3.1. The Transfer of Customer Confidential Information

The recent amendment to the Banking Law[50] defines customer confidential information in Article 73. Accordingly, all the data relating to real and legal persons generated after establishing a customer relationship with banks for banking activities are deemed as customer confidential information. The definition of customer confidential information excludes the data collected due to non-banking activities[51] and the information obtained from non-customers. The customer confidential information covers personal data and non-personal data.

Customer confidential information can only be transferred to third parties abroad or within the country upon specific instructions or requests of the customer. The provision clearly states that customer's explicit consent, obtained according to PDPL, is not sufficient to transfer customer confidential information to third parties within the country or abroad. The mandatory legal provisions in other laws, audits, court requests, and information that must be disclosed to some specific ministries were specified as exemptions.

Customer confidential information can only be transferred if it is limited to the stated purposes and is exclusively restricted to attaining the objectives. Article 10 of the Banking IT Regulation repeats the content of Article 73 of the Banking Law, which restricts the transfer of customer confidential information to third parties located within the country or abroad. However, BRSA is authorized to prohibit the transfer of customer confidential information as a result of an evaluation based on

[50] Amendment on Banking Law and other laws 2020 Article 10.
[51] The banking activities were specified on Article 4 of Banking Law. For example providing insurance to customers or purchasing land/property is a non-banking activity, whereas credit lending would be deemed as banking activity.

economic security, with third parties abroad. There is no restriction for the time being.

3.1.3.2. System Localization

Despite the fact that the banks are not required to install their primary and secondary systems within the country according to the Banking Law, BRSA was authorized to oblige the banks to keep their primary and secondary systems within the country.

According to Article 25 of the Banking IT Regulation, banks must keep all their primary and secondary systems within the country. The primary system refers to all kinds of infrastructure, hardware, software, and data of the banks, and the secondary system relates to the backups of the primary system, which aids in the continuity of operations in case the primary system fails.

All kinds of backups will be deemed secondary systems no matter how many there may be. Systems like internal messaging and market tracking platforms that do not aim to fulfill the responsibilities set forth with the relevant regulations are excluded from primary systems. Yet, these systems must not contain any sensitive data[52] or confidential information, nor must be used for business operations to be deemed as an exception for primary systems. The primary and secondary systems of the banks must not be dependent on a system installed abroad, and all business operations installed within the country must be sufficient for continuing banking services. Thus, the information systems used by an external service or cloud computing providers must also be installed within the country.

[52] Banking Regulation and Supervision Agency Regulation on Banks' Information Technology and Electronic Banking Services (n 5). 3/o - Sensitive data is defined primarily as data used in authentication, which belongs to the customer and is kept by the bank for various reasons, and if they are seized by third parties, their mechanisms of discrimination with those who are customers will be damaged and may result in fraud or fake transactions on behalf of customers.

In practice, most of the primary systems are installed within Istanbul, and the secondary systems are installed in Izmir or Ankara due to provide business continuity.

3.1.3.3. Bank Receipts and Local Production

According to Article 37/8 of the Regulation, the banks must send all kinds of documents such as receipts and statements, which contain sensitive data through electronic banking service channels. Accordingly, it is the banks' responsibility to lead customers to use electronic distribution channels for receiving such documentation. The banks started to inform their customers, according to Article 37/8, that receiving their statements and financial information from their e-mail addresses are less secure than the banking channels since the data at the mail addresses are stored abroad.[53] Various international financial institutions also use this method.[54]

The local production of the services/products of the external service providers in the fields of critical information systems and security was indicated as a vital selection criteria according to Article 29 of the Banking IT Regulation. Having an R&D center in Turkey was also specified as selection criteria.

3.1.3.4. Sanctions

Article 159 of Banking Law indicates that the responsible ones who violate Article 73, the conditions set for the transfer of customer confidential information, can face one to three years of imprisonment and a judicial fine between one and two

[53] Yapıkredi, 'E-Posta Gönderimlerindeki Değişiklikler Hakkında Bilgilendirme' (2020) <https://www.yapikredi.com.tr/e-posta-bilgilendirme> accessed 28 August 2020.
[54] Interactive Brokers also offers its client a secure delivery preference to receive such notifications.

thousand days. Before the recent amendment, Article 159 was in force, but it is still applicable for violating the transfer of customer confidential information due to the wording. Also, according to Article 148 of Banking Law, BRSA can impose administrative fines.

3.1.4. Analysis of the Legal Framework

3.1.4.1. Definition of Financial Data

PDPL specifies personal data and special category of personal data. Health data, political belief, trade union, and association membership data are specified as special category of personal data. Financial Data was not specified in either category of data, thus, every financial data must be evaluated based on the nature, and the requirements must be fulfilled accordingly. For example, association membership payment data must be evaluated as a special category of personal data since it reveals the association membership of the data subject, while regular e-commerce payment data must be deemed as personal data. Categorizing all the payment data would be an immense burden for financial institutions, and it is clear that the structure is not fit to meet the needs of the financial sector.

The Banking Law defines customer confidential information as all the data generated after the customer relationship is established for banking activities. The broad definition simplifies the process for banks. However, despite the fact that customer confidential information covers all the personal data of the customers, the banks may also have personal data of non-customers or may have personal data processed as a result of the non-banking activity for various reasons. Thus, the definition of customer confidential information does not contain all the personal data that the banks keep, and the definitions in PDPL must also be considered while categorizing the information.

3.1.4.2. Processing Grounds

The Banking Law and the Payment Law does not specify on what basis the entities can process data. Thus, PDPL must be examined. Most of the data processed by the financial institutions is related to their customers and are processed as a result of the execution of a contract. Therefore, explicit consent is not required to process the data since the execution of a contract is counted as one of the legal basis to process data without the explicit consent of the data subject. However, sometimes the processed data can be deemed as a special category of personal data, or it can be the data of a silent party that does not have any contractual relationship with the financial institutions. Then, the processing can be based on "legitimate interest " or "provided by the law" basis since the financial institutions must keep the records of the payments, money transfers, etc. according to the relevant laws. Yet the processing of third party data should be strictly limited to the purpose and should not be further processed for any other purpose.

3.1.4.3. Local Processing

Apart from being a bank or payment service, the financial institutions are obliged to process and store data within Turkey, which can be defined as Local Processing. The Local Processing requirements prevent the Banks, payment service, and e-money institutions from using Public Cloud or data centers abroad.

Only the systems of internal messaging and market tracking platforms of banks that do not aim to fulfill the responsibilities set forth with the Banking provisions and does not contain sensitive data can be installed abroad. Hence public cloud services could also be retained for these platforms. There are no exemptions for payment services and electronic money institutions.

The local processing requirement for payment services and e-money institutions was introduced with Payment Law, and besides requiring the entities to install their

primary and secondary systems inside Turkey, all of their documents and records must be stored in an accessible and secure manner for at least ten years inside Turkey. The violation of local processing requirements may result in the cancellation of the license, imprisonment up to 3 years, and a judicial fine of one thousand five hundred days for responsible individuals.

Despite the localization requirement brought by Payment Law (primary legislation), the Banking Law authorizes BRSA as the competent authority to decide if the banks have to install their information systems and backups inside Turkey or not (secondary legislation). Accordingly, BRSA obliges the banks to install their information systems and back-ups inside Turkey.

3.1.4.4. Restrictions on Transferring Data Abroad

Payment Law indicates that the documents and records must be kept at domestically installed information systems and their backups. Although the requirements clearly state that the data must be stored locally at primary and secondary systems with an extensive definition of these systems, there are no rules that ban the transfer. Thus, PDPL, as the primary data protection law, can be a resort to be referred to fulfill the gap in transferring data. Accordingly, the payment services and e-money institutions must satisfy at least one of the four requirements stated at PDPL, in which explicit consent is the only applicable method for the time being.

The Banking Law goes one step further than PDPL, making it more complicated to transfer data abroad. Accordingly, even if the data subject's explicit consent is obtained according to PDPL, the customer confidential information cannot be transferred unless the specific instructions or request of the customer is received. The Banking Law separates the explicit consent of PDPL from the customer's specific instructions and requests. The reasoning of Article 73 submitted by the ruling Party indicates that Article 73 is lex specialis in terms of the transfer of

customer confidential information[55] and thereby prevails PDPL Article 9. The Turkish DPA also indicated that Article 73 of Banking Law must be applied for cross border data transfers according to Article 9/6 of PDPL, whereas the general principles of PDPL are still relevant[56]. However, the cross-border transfer of personal data that does not fall under the definition of customer confidential information must be carried out according to Article 9 of PDPL.

The recent amendment on Article 73, introducing customer confidential information, was brought in line with open banking developments. BRSA aims to create a compelling and secure data transfer regime for banks and other financial institutions that are getting prepared for open banking. However, the extensive definition of customer confidential information covers nearly all types of data relevant to the customers and banking activities, i.e. customer name and account number. Thus, even the customer name transfer will be subjected to the requirements stated in Article 73, which would be an immense burden for banks and restrict non-sensitive personal data.

3.1.4.5. Sanctions

Three strong authorities overlap on personal data matters. The DPA is authorized to monitor all kinds of personal data matters and is eligible to grant any decisions based on the PDPL. The BRSA is entitled to enforce the Banking Law that contains provisions on storing, processing, and transferring data and fines, measures, and punishments. The Central Bank is responsible for payment services and electronic money institutions due to a power shift from BRSA.

Central Bank is entitled to cancel the license of payment and electronic money providers and submit a complaint against the individuals who violate Article 23 of

[55] Justice and Development Party (AK Parti), The Reasoning of Amendment Law 2020 Article 10.
[56] Turkish Data Protection Authority, 'Announcement on Cross-Border Transfer' (2020) <https://kvkk.gov.tr/Icerik/6828/YURTDISINA-VERI-AKTARIMI-KAMUOYU-DUYURUSU> accessed 29 October 2020.

Payment Law. According to Article 23 of Payment Law, the payment services and electronic money institutions must keep all of their documents and records in an accessible and secure manner for at least ten years within Turkey. For example, if the payment service provider erases the data in line with the request of the customer according to PDPL before ten years, despite acting according to PDPL, Article 23 of Payment Law will be violated, and the responsible person might be subjected to an imprisonment of up to three years. Besides, if the payment provider does not keep the data by taking the necessary security measures according to Article 23 of Payment Law and Article 12 of PDPL, this will violate both provisions. Since there are no rules at Payments Law regarding the cross border transfers of personal data, the DPA will continue to influence the practice of payment services and e-money institutions on cross-border data transfers unless separate regulations will be introduced.

BRSA is entitled to impose administrative fines on Banks who do not comply with the Banking Law or regulations issued under the Banking Law and can file complaints against the individuals to the Prosecutors' Office according to Article 159 that may result in their imprisonment if found guilty. For example, supposing that Bank A transferred the customer confidential information, i.e., the customer name, to a third party, with the explicit consent of the data subject obtained according to Article 9 of PDPL, the bank might be subjected to an administrative fine and the individual responsible for the incompliant transfer might face imprisonment, since the written instructions or request of the data subject was not obtained according to Article 73 of Banking Law.

The incompliant transfer of personal data within the scope of PDPL might be subject to administrative fines under the PDPL and criminal sanctions under the Turkish Criminal Law[57]. The definition of customer confidential information and detailed provisions on storing, processing, and transferring data, including the proportionality and purpose limitation clause in the Banking Law, decreases PDPL

[57] Direnç Bada and Begüm Okumuş Yavuzdoğan, 'Turkey's New Data Storage and Transfer Requirements for Banks' (*iapp*, 2020) <https://iapp.org/news/a/turkeys-new-data-storage-and-transfer-requirements-for-banks/> accessed 2 October 2020.

and DPA's influence on banks. Despite that Article 73 of Banking Law prevails Article 9 of PDPL and BRSA is entitled to monitor the cross-border data transfers of Banks, since the general principles of PDPL are still applicable, DPA might also intervene in matters related to cross-border data transfers of Bank and can influence the practice of Banks.

3.2. EUROPE

Europe acknowledges the importance of data flow and its meaning for the new technologies such as IoT and AI. Thus, it forbids its member states to implement data localization rules on non-personal data unless public security reasons justify it[58]. The same restriction applies to personal data. According to Article 1 of General Data Protection Regulation (GDPR),[59] *"The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."*

Europe sets conditions for transferring personal data outside the Union. Thus, financial institutions, including banks and payment services, can transfer, store, and process data abroad by complying with the rules in GDPR. There are no other regulations that may force entities to keep the data within the European borders. Yet, the European Banking Authority (EBA) urges financial institutions to take

[58] European Union, REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union 2018 1." Paragraph 18 *"Data localisation requirements represent a clear barrier to the free provision of data processing services across the Union and to the internal market. As such, they should be banned unless they are justified on grounds of public security, as defined by Union law, in particular within the meaning of Article 52 TFEU, and satisfy the principle of proportionality enshrined in Article 5 TEU. In order to give effect to the principle of free flow of non-personal data across borders, to ensure the swift removal of existing data localisation requirements and to enable, for operational reasons, the processing of data in multiple locations across the Union, and since this Regulation provides for measures to ensure data availability for regulatory control purposes, Member States should only be able to invoke public security as a justification for data localisation requirements*.

[59] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

location into account as part of their risk-based approach[60], so they might decide not to locate data outside of Europe as part of their internal policy.

According to the European Banking Authority data, 67% of the banks in Europe use cloud in storing and processing data, up from 55% in 2018. The other %11 is under pilot testing, 11% is under development, and the remaining 11% is under discussion.

The survey held with 41 EU banks by Bloomberg Businessweek reveals that 15 banks are using Microsoft Azure, 10 are using AWS, 7 Google, 6 IBM, 2 Salesforce, and 1 NetApp, meaning that the customer data of the European banks are all kept at public cloud servers of US Companies[61]. Although there are concerns around US Cloud Act[62] and privacy-related issues, the numbers of European banks

[60] European Banking Authority, Recommendations on outsourcing to cloud service providers 2017 1 17. Paragraph ***4.6 Location of data and data processing;*** *19. As stated in guideline 4(4) of the CEBS guidelines, institutions should take special care when entering into and managing outsourcing agreements undertaken outside the EEA because of possible data protection risks and risks to effective supervision by the supervisory authority.; 20. The outsourcing institution should adopt a risk-based approach to data and data processing location considerations when outsourcing to a cloud environment. The assessment should address the potential risk impacts, including legal risks and compliance issues, and oversight limitations related to the countries where the outsourced services are or are likely to be provided and where the data are or are likely to be stored. The assessment should include considerations on the wider political and security stability of the jurisdictions in question; the laws in force in those jurisdictions (including laws on data protection); and the law enforcement provisions in place in those jurisdictions, including the insolvency law provisions that would apply in the event of a cloud service provider's failure. The outsourcing institution should ensure that these risks are kept within acceptable limits commensurate with the materiality of the outsourced activity.*

[61] Justina Lee, Steven Arons and Nicholas Comfort, 'European Banks Store Their Sensitive Data on American Clouds' (*Bloomberg Businessweek*, 2020) <https://www.bloomberg.com/news/articles/2020-03-06/european-banks-store-their-sensitive-data-on-american-clouds?utm_source=url_link>.

[62] Clarifying Lawful Overseas Use of Data (CLOUD) Act enacted in 2018 empowers the US Government to access data from American companies regardless of the data's location. Thus, whether the data is stored in a third country or inside the US, the American companies would have to comply with the US Court's data request. This law was passed during a pending court file, originated from Microsoft's rejection of a US Magistrate Judge's data request. Microsoft claimed that the Court had a territorial limit and could not request the data held in Microsoft's data center in Ireland. After the establishment of the US Cloud Act, Microsoft complied with the request. US Cloud Act extends the US power to reach the data located in third countries and creates a separate tool other than the MLAT process. Thus, the US Court can request data from all American companies worldwide by bypassing the MLAT or other formal procedures even if the request contradicts the law of domestic countries. However, third countries would still have to rely on MLAT or rogatory letters to request data located in the US unless they are authorized with an executive agreement. To sum up: According to the US Cloud Act, US Courts can directly request

using public cloud servers are increasing every year at high speed due to the virtue of cloud servers in decreasing the costs of data storing and processing, the SaaS that are provided for the business, and keeping up with the competition with fintechs and other banks.

This section will review the GDPR and PSD2 in respect of processing, storing, and transferring data.

3.2.1. General Data Protection Regulation (GDPR)

The primary legislation for personal data protection is found in Article 16 and Articles 7 and 8 of the EU Charter of Fundamental Rights. Article 6 TFEU stipulates that everyone has the right to the protection of their personal data. Current EU legislative instruments on data protection are now found in GDPR as secondary legislation. GDPR entered into force across the EU on May 25, 2018. Since then, all organizations within the EU Member States, EU based individuals, and companies that target the EU consumers are expected to comply with GDPR.

One of the main goals of GDPR is to unify personal data protection across European countries, enable the free flow of data by providing safeguards and protecting the

Microsoft to share the data located in Microsoft's data center in France, but France cannot directly request the data in the U.S unless they sign an executive agreement with the US. As of 2021, UK is the only country with an executive agreement with the US. See the details of the US Cloud Act and its application: "Hemmings, Justin and Srinivasan, Sreenidhi and Swire, Peter, Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act (October 7, 2019). Journal of National Security Law and Policy, Forthcoming, Georgia Tech Scheller College of Business Research Paper No. 3469808, Available at SSRN: https://ssrn.com/abstract=3469808" Some argue that this law would be a reason for numerous localization laws around the world. See: "Paul Schwartz and Peifer Karl-Nikolaus, 'Data Localization Under the CLOUD Act and the GDPR' (2019) 1 Computer Law Review International. Some say that this law will damage the privacy of foreigners and American citizens. See: "Secil Bilgic, 'SOMETHING OLD, SOMETHING NEW, AND SOMETHING MOOT: THE PRIVACY CRISIS UNDER THE CLOUD ACT' (2018) 32 Harvard Journal of Law & Technology."

citizens. GDPR identifies two different categories of personal data; personal data and special category of personal data.

The definition of personal data in the GDPR is:

"*Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who ben identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*[63]

Data is personal if the person's identification is possible based on the available data, i.e., if a person can be detected, directly or indirectly, by reference to an identifier. This can be the name, identification number, card number, or location data. Therefore, information is not considered personal data if it is impossible to link it to a natural person.[64]

"Special category of personal data" are specified as:

"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Financial data is not indicated as Special category of personal data; thus, it must be evaluated for every specific data, whether it falls under its scope. For example, the payment to a religious institution might be classified as a special category of personal data, whereas the regular e-commerce payment data must be deemed personal data. Despite differences in processing personal data and special category

[63] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. Article 4/1.
[64] Paul Voigt and A Von dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Springer 2017) 11.

of personal data, the cross-border data transfer regime to and outside of the European Economic Area is the same.

GDPR allows the free flow of personal data between member states without any restriction. However, transfers of personal data to any country out of the European Economic Area can only be conducted by certain conditions.

Initially, the data must be lawfully processed, and the transfer purpose must be in line with the processing purpose. Then, at least one of the below conditions set forth under the GDPR Chapter V must be met.

- The third country/territory must be determined as adequate for the protection of the personal data by The European Commission,[65]
- If the Commission does not recognize the country that the transfer will be made as an adequate country, the controller or processor must take the appropriate safeguards such as standard contractual clauses or binding corporate rules,
- If the country is not adequate and the appropriate safeguards do not exist, personal data transfers must be legalized with one of the derogations, including compelling legitimate interest pursued by the controller and explicit consent of the data subject. The derogations are not fit for continuous data transfers and could only be used for particular transfers.

Recital 101 of GDPR highlights the importance of the personal data flows to and from countries outside the European Union to expand international trade and cooperation, thus the world economy. However, the significance of the measures is also highlighted to retain the level of protection of natural persons brought with the Regulation, and the aim is not to block the flow of data unless the protection level is not provided. GDPR expects a similar protection level from other countries as it gives, and *Ustaran* pointed out that this creates a situation that effectively imposes

[65] Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay, were determined as adaquate and adequacy talks are ongoing with South Korea. Please see European Commission, 'Adequacy Decisions' <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>.

EU data protection standards in jurisdictions outside of Europe[66]. The extend of the influence could be understood by looking at many countries that are implementing similar rules. Even China's draft PDPL contains many provisions similar to the ones at GDPR[67].

United States of America (limited to the Privacy Shield framework) was also deemed as a safe country and most of the transfers to the US from the EU were carried out based on the EU-US Privacy Shield Framework. However, the European Commission's adequacy decision for the EU-US Privacy Shield Framework was invalidated with the decision of the Court of Justice of the European Union (Schrems II)[68], and the international transfers carried out based on the privacy shield was prohibited. Thus, some of the European authorities started to implement tougher rules by extending the decision's application, which is seen to be conflicting with the GDPR.

For example, in a case where Microsoft Azure's suspension was requested for hosting the data of the French health data platform, French Data Protection Authority (CNIL) suggested that US Cloud providers must not be used for hosting health data. CNIL states that whether the data is inside or outside Europe, since the US providers fall under FISA702 and other US surveillance laws, they should not be used[69]. Although CNIL indicated that this position only concerns health data and "it reserves its position on other sectors and other, less sensitive, categories of data," its reasoning could be transposable to other categories of personal data in the future. Despite the strong recommendation of CNIL, the French Administrative Supreme Court did not rule the suspension and concluded that the Schrems II ruling does not mean that processing by a US provider in the EU territory is in itself a violation of

[66] Eduardo Ustaran, *European Data Protection Law and Practice* (International Association of Privacy Professionals (IAPP) 2018) 239.
[67] Gil Zhang and Kate Yin, 'A Look at China's Draft of Personal Data Protection Law' (*iapp*, 2020) <https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/> accessed 30 October 2020.
[68] *PRESS RELEASE No 91 / 20 The Court of Justice invalidates Decision 2016 / 1250 on the adequacy of the protection provided by the EU-US Data Protection Shield* (2020) C-311/18.
[69] Romain Dillet, 'France's Health Data Hub to Move to European Cloud Infrastructure to Avoid EU-US Data Transfers' (2020) <https://techcrunch.com/2020/10/12/frances-health-data-hub-to-move-to-european-cloud-infrastructure-to-avoid-eu-us-data-transfers/> accessed 13 October 2020.

the law[70]. Yet, the Court required Microsoft to take the safeguards to prevent the EU-US transfers.

The EU officials repeat that they do not see data localization as a data protection measure and will not support a general trend towards data localization. However, current developments such as the CNIL recommendation show us that there is a tendency to apply stricter rules that exceed data protection purposes.

3.2.2. Payment Service Directive 2 (PSD2)

The objective of PSD2 is to harmonize the regulatory framework of the internal market for electronic payments in the EU. PSD2 sets out detailed rules on payment services intending to make payments simple, efficient, and secure for all Member States and set a unified practice. Also, efforts are being made to open the payment market for new parties to increase competition and diversify customer choice. Thus, the introduction of PSD2 is expected to increase the use of payment services and competition by making it easier for third-party service providers (TPPs) to compete with banks in providing payment services.

PSD2 enables consumers and sellers to use TPPs, such as fintech companies, to manage their finances. The TPPs must be registered as Account Information Service Provider (AISP) or Payment Initiation Service Provider (PISP) to conduct business. PSD2 enables payment service providers to access the user's bank account information with their prior consent to offer innovative services. The banks must share such information as soon as they verify the explicit consent of the customer.

[70] Patrice Navarro, 'French Court Refuses to Suspend Microsoft's Hosting of a Public Health Data Lake despite CNIL Opinion' (*Hogan Lovells*, 2020) <https://www.engage.hoganlovells.com/knowledgeservices/news/french-court-refuses-to-suspend-microsofts-hosting-of-a-public-health-data-lake-despite-cnil-opinion-the-health-data-hub-case-part-2> accessed 29 October 2020.

3.2.3. The relation between GDPR and PSD2

While PSD2 is intended to improve competition and innovation in the internal market, the GDPR, on the other hand, aims to protect all EU citizens from privacy and data breaches in an increasingly data-driven world. The perspective behind each Regulation is very different. PSD2 establishes a way to access the personal data and obliges its sharing, while GDPR operates to regulate and safeguard it. This raises compliance considerations on how to apply them together and ensure innovation while protecting the data.

According to PSD2, traditional payment service providers such as banks will need to share specific data, like payment data, with TPPs upon the customer's explicit consent. Payment data will identify the customer so that it will be under personal data protection by GDPR. This can create a conflict between payment service providers being ordered to share personal data by PSD2 while simultaneously regulating such sharing under GDPR[71].

Article 94 of PSD2 states that the processing of personal data concerning PSD2 must comply with GDPR; moreover, it states that TPPs, shall only access, process, and retain personal data necessary to provide their payment services, with the explicit consent of the payment service user.

TPPs, access to accounts are provided for in Articles 66 and 67 of PSD2. Accordingly, with the explicit consent obtained under PSD2, TPPs can request access to their customers' payment accounts'. PSD2 does not mention the need for banks to obtain the consent of customers before providing TPPs with access to customer payment accounts through banks' application programming interfaces (APIs). However, TPPs must have customer's explicit consent in place to ensure that their access to bank account information and payments made on their

[71] Dilja Helgadottir, 'THE INTERACTION BETWEEN DIRECTIVE 2015/2366 (EU) ON PAYMENT SERVICES AND REGULATION (EU) 2016/679 ON GENERAL DATA PROTECTION CONCERNING THIRD PARTY PLAYERS' (2020) 23 Trinity College Law Review 201, 215.

customers' behalf are fully compliant. The TPP can then process the information request to the correspondent bank, and the bank's role is to verify whether the customer's explicit consent obtained by the TPP is in line with the requirements[72]. To conclude, the payment service providers must first obtain the customer's explicit consent and simultaneously comply with the conditions of GDPR to transfer the data outside Europe.

3.3. COMPARING TURKEY AND EU

Turkey closely observes the practice of Europe concerning personal data and information technology policies. Especially the Data Protection Directive 95/46 of Europe had a significant influence on Turkey's PDPL. Turkey's pursuance seems to continue since Turkey's 11th Development Plan sets objectives for the PDPL's amendment according to the GDPR[73]. However, there are significant differences regarding the data policy towards financial institutions and personal data practice.

Firstly, Europe does not impose any localization requirements on Banks, payment services, or electronic money institutions, while Turkey implements strict localization rules requiring the banks, payment, and electronic money providers to install all their systems within Turkey. Thus, most European financial institutions enjoy the benefits of cloud and SaaS, and Turkish financial institutions are barred from using them.

Secondly, Banking Law is *lex specialis* to the PDPL regarding the customer confidential information transfer. Considering the broad definition of customer confidential information, the Banks may only transfer the data based on the customer's specific instructions or request, and the other methods stated at PDPL

[72] Dilja Helgadottir, 'The Conflict Concerning Data Sharing under PSD2 and Obtaining Consent to Share Such Data under GDPR' (*University of Oxford Faculty of Law*, 2020) <https://www.law.ox.ac.uk/business-law-blog/blog/2020/07/conflict-concerning-data-sharing-under-psd2-and-obtaining-consent> accessed 4 October 2020.
[73] Presidencey of the Republic of Turkey, '11th Development Plan' (2019) 479.1.

would not apply for cross-border transfers. In contrast, the PSD2 adds an additional requirement for payment services to obtain the explicit consent of the customer to transfer the personal data and the cross-border transfer conditions in the GDPR still apply.

Thirdly, despite the different intentions, PSD2 and GDPR are in harmony and complete each other. However, the relationship between Turkey's PDPL, Banking Law, and Payment Law overlaps in many respects, such as storing and transferring data, the role and involvement of the regulative bodies (please see section 3.1.4.). While PSD2 states that the payment providers must be compliant with GDPR, the Banking Law does not refer to the PDPL in any of the provisions and clearly excludes the terms in PDPL, creating an ambiguous situation for personal data transfers.

Fourthly, the Banking Law empowers the Banks to obtain the written instructions or request of the customer, while the PSD2 empowers TPPs in receiving the explicit consent and requires the Banks to verify whether the customer's explicit is accurate. The open banking provisions in Turkey are divided into Payment Law and Banking Law, and there is no unified approach.

Fifthly, PDPL applies the cross border transfer rules based on how it is processed. If the data is processed based on the data subject's explicit consent, then the only way to transfer the data abroad is to obtain the data subject's explicit consent. However, GDPR sets rules for transferring data abroad apart from the processing method.

Lastly, one of the primary objectives of GDPR is to ensure the free flow of data and had established a multi-alternative mechanism to facilitate the transfer of data by providing more opportunities for cross-border data transfer. Explicit consent is used as one of the last remedies for cross-border data transfer and was regulated under the heading "deregulations." PDPL also has different cross-border transfer methods, but the only available method for the time being is to obtain the data subject's explicit consent. The lack of cross-border transfer methods forces the

entities to keep their data at locally installed data centers, which contradicts one of the main objectives of GDPR – free flow of data.

3.4. OTHER COUNTRIES

3.4.1. India

According to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules (IT Rules),[74] financial information such as Bank account or credit card or debit card, or other payment instrument details are deemed as sensitive data. According to Article 7, sensitive personal data could be transferred to any other country that ensures the same level of data protection by obtaining the data subject's consent. The consent is not necessary for the transfer if it is required for the performance of a lawful contract between the corporate entity and the data subject. However there are special rules for financial institutions in respect of payment data.

The Reserve Bank of India ("RBI") announced that all data related to payment systems should be stored within India, and the violation may result in the cancellation of the license to operate as a Payment System.[75] RBI clarified that payment transactions could be processed outside India. However, the data shall be stored only in India after the processing ends. In case the processing is carried out abroad, the data should be deleted from the systems and brought back to India not later than the one business day or 24 hours from payment processing.[76]

[74] MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY Department of Information Technology, 'Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011' <https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>.
[75] Reserve Bank of India, 'Storage of Payment System Data' 1 <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF>.
[76] Reserve Bank of India, 'Reserve Bank of India - Frequently Asked Questions' <https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130> accessed 28 August 2020."

Since banks function as operators of a payment system or as a participant in a payment system, they also must store all their data in India. However, according to RBI, foreign banks can continue to store the banking data abroad as long as the domestic payment transactions are stored within India[77].

The RBI decision on Payment System Data raised the concerns of companies like PayPal, Visa, MasterCard, and American Express, whereas domestic companies such as Jio supports it[78]. Despite the opposition, Mastercard has started storing all its payments transaction data in the western city of Pune, yet it is not clear whether a copy of that data was still being stored abroad[79].

According to the survey of the Centre for Internet and Society[80], the supporters of the localization rules indicates that the rules will help to combat the anti-money loundering scenes, will establish a more secure financial sector, ensure the access of data by courts, promote data sovereignty and prevent the data colonialism led by global corporations. The critics of data localization in India state that the rules will hinder innovation and investment, increase the costs of services for businesses and customers, disrupt existing business models, prevent startups from entering the global arena, and put burden by installing data centers to the Indian energy market. The opposers also claim that concerns related to the protection, security, and access to data could be addressed using alternative methods.

[77] "ibid Question 9.
[78] Ronak D Desai, 'India's Data Localization Remains A Key Challenge For Foreign Companies' (*Forbes*) <https://www.forbes.com/sites/forbesleadershipteam/2020/08/10/business-as-unusual/#6e38931a24d5>.
[79] Aditya Kalra, 'Mastercard Says Storing India Payments Data Locally in Face of New Rules' (*Reuters*, 2018) <https://cn.reuters.com/article/india-data-localisation-mastercard-idCNL3N1XA5JH>.
[80] Arindrajit Basu, Elonnai Hickok and Aditya Singh Chawla, 'The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India' [2019] The Centre for Internet and Society 75–92 <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf>.

3.4.2. China

The Cybersecurity Law of China, which took effect in 2017, requires the financial institutions and other critical information infrastructure (CII) to store personal information and important data collected and generated during operations within China[81]. Important data is defined as "data that, if divulged, may directly affect national security, economic security, social stability, or public health and safety, such as undisclosed government information or large-scale data on the population, genetic health, geography, mineral resources, etc."[82] For real business necessity, the CII operator, including financial institutions, may transfer the important data abroad after being subjected to a security assessment.[83] The Cybersecurity Law provides that the operators of the CII would be subject to the local data residency and safety assessment requirements should they transfer such data abroad.[84]

In line with China's Cybersecurity Law, the People's Bank of China (PBOC) issued the Technical Specification for Protection of Personal Financial Information (the "PBOC Specification") on 13 February, 2020. The PBOC Specification is a recommendation for financial institutions and has no enforceable nature.

Personal Financial Information (PFI) is defined as "any personal information collected, processed and stored by Financial Institutions during the provision of financial products and services," and PFI was degreed into three categories based on its sensitivity: C3, C2, and C1.

---

[81] Rogier Creemers, Paul Triolo and Graham Webster, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' (*New America*, 2018) Article 37 <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/> accessed 28 August 2020.

[82] Katharin Tai and others, 'Translation: China's New Draft "Data Security Management Measures"' (*New America*, 2019) Article 38 <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/> accessed 28 August 2020.

[83] Yuxi Wei, 'Chinese Data Localization Law: Comprehensive but Ambiguous - The Henry M. Jackson School of International Studies' (2018) <https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/> accessed 28 August 2020.

[84] HFW, 'China: Cybersecurity Law and Data Localisation - Lexology' (2018) <https://www.lexology.com/library/detail.aspx?g=ee05d71c-fe7f-44ca-87ce-6ae0afb74071> accessed 18 May 2020.

C3 refers to "financial information whose unauthorized use or alteration will cause significant harm to data subjects." C2 refers to "financial information that can point to an identifiable individual." C1 refers to "personal information used by financial institutions internally and is less sensitive than C3 and C2 categories"[85]. Different security standards are required for the protection of each category[86]. However, the strict localization requirement brought with Cybersecurity Law obliges the financial institutions to store, process, and analyze the data within China. As an exception, if real business necessities requires the cross border transfer, the Financial Institution must first obtain the explicit consent from Data Subjects, conduct a security assessment, and then supervises the offshore recipient to ensure responsible processing, storage, and deletion of PFI with a contract or an on-site inspections[87].

China introduced its draft Personal Data Protection Law, which is still under public consultation. There are similar provisions with the GDPR. However, the data localization requirement put forward with Cybersecurity Law remains in the draft PDPL. Accordingly, CII operators, which processes over certain amounts of personal data in China, are obliged to keep the data within China. Besides, the rules for cross border transfers were clarified, and specific methods were introduced for enabling data transfers. These are (i) obtaining authorization, (ii) cross-border data transfer agreements signed with the recipient, (iii) other mechanisms stated in other laws and regulations. Regardless of the transfer method, the data subject's consent must be obtained to transfer the personal data abroad, and any cross-border data transfer is subject to security assessment to be conducted by the Chinese regulators[88].

[85] personal information which does not fall into categories C2 and C3.
[86] Norton Rose Fulbright, 'PBOC Issues New Specification on Personal Financial Information' (*March*, 2020) <https://www.nortonrosefulbright.com/en-gb/knowledge/publications/fcdc5f10/pboc-issues-new-specification-on-personal-financial-information> accessed 28 August 2020.
[87] Linklaters, 'PBOC Publishes New Data Protection Guidelines for Financial Institutions' (2020) 3 <https://e.linklaters.com/67/921/downloads/20200304-pboc-publishes-new-data-protection-guidelines-for-financial-institutions.pdf>.
[88] Zhang and Yin (n 67).

3.4.3. Russia

Russia is the largest economy that implements a data localization requirement for all sectors[89]. Russia introduced Federal Law FZ-152, also known as the On Personal Data Law (OPD Law). It contains similar provisions to those in the Data Protection Directive 95/46 of Europe and has been in force since January 26, 2007. In July 2014, the Russian OPD Law was amended by FZ-242 and includes data localization requirements. FZ-242 Article 18/5 requires data operators to store and process Russian citizens' personal data in databases installed inside Russia. If not, the Roscomnadzor (Russia's DPA) is entitled to block the websites.

Although there is a localization requirement, transferring personal data outside Russia to adequate countries is possible. All of the states ratified the Convention 108 are deemed safe, and besides the Member States of the Convention, 23 more states were included in the safe country list.

If the personal data transfer is carried out to one of the countries out of the list, a cross border transfer is permitted if one of the following conditions is met[90]: (i) Data subjects consents, (ii) Performance of a contract to which the data subject is party; (iii) Provided by an international treaty in which Russia is a signatory, (iv) For the protection of the constitution, state defense, security, and transport system per federal laws and (v) Protection of the data subject's vital interests where it is not possible to get data subject's written consent.

3.5. ANALYSIS

As a result of the above examination, Russia, China, and Turkey adopts local processing for the financial institutions. Accordingly, all the storing and processing

[89] Matthias Bauer and others, 'Data Localisation in Russia: A Self-Imposed Sanction' (2015) 2.
[90] DLA Piper, 'DATA PROTECTION LAWS OF THE WORLD' <https://www.dlapiperdataprotection.com/index.html?t=law&c=RU&c2=TR>.

activities must be held within the said countries. However, as an exception, India allows the financial institutions to process the data abroad by obliging them to delete the data and bring it back to India within one business day or 24 hours, starting from the payment processing time. (Table 3.1)

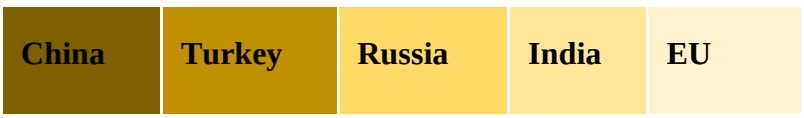
However, concerning the cross border transfers, there are differences for each country. While China makes it very hard to transfer the data abroad, EU member states, Russia, India, and Turkey provide possible methods to transfer the personal data. Yet, the requirements also vary based on the methods that are available to send the data abroad. The most challenging conditions were set for Chinese and Turkish financial institutions. (Table 3.1) (Figure 3.2)

Table 3. 1 Data Localization Practices for Financial Institutions

COUNTRY	LOCAL STORAGE	LOCAL PROCESSING	CROSS BORDER TRANSFER
CHINA	Yes	Yes	Very Hard
TURKEY	Yes	Yes	Hard
RUSSIA	Yes	Yes	Medium
INDIA	Yes	No	Medium
EU	No	No	Medium

Source: Primary and secondary legislation of the selected countries

Figure 3. 2 Data Localization Degree



Source: Primary and secondary legislation of the selected countries

SECTION 4
ECONOMIC ANALYSIS OF DATA LOCALISATION RULES

4.1. MACROECONOMIC ANALYSIS

According to some economists, data flows are among the most significant opportunities for the developing countries to narrow the gap with the developed countries, considering that the trade of tangible goods was mostly exchanged between the developed countries, and the global data flow promises greater participation of developing countries.[91]

In this section, the reports that quantify the economic impact of localization rules to export, import, production, GDP, welfare, investment, FDI, job creation, and energy market will be examined and analyzed.

4.1.1. The impact on the national economies

4.1.1.1. Chatham House Report[92]

In this report, the economic impact of the data localization requirements were analyzed by focusing on the existing regulations and data intensity for sectors of the selected countries. The study used two different variables, Total Factor Productivity (TFP) and Process Value Analysis (PVA).

TFP indicates whether an economy is growing because of an increase in capital or labor or because those inputs are being used more efficiently, which technology and

[91] Mckinsey Global Institute (n 1) 15.
[92] Matthias Bauer, Martina F Ferracane and Erik Van Der Marel, 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization'.

innovation are the main drivers.[93] According to the famous economist, Robert M. Solow, the main driver of the labor productivity between 1909-49 in the United States was the developments in the technology rather than capital spending. Accordingly, only one-eighth of the increase could be attributed to a conventional increase in capital intensity, while the other seven-eight was for "technical change in the broadest sense."[94] TFP was chosen as a measure since more regulations will make it harder and costly for firms to adopt, resulting in lower productivity.

PVA determines the unnecessary steps and expenses incurred in the value chain that can be eliminated without lowering customer expectations[95]. The implementation of new technologies is one of the key factors in reducing costs and eliminating unnecessary processes.

The report highlights that data localization rules will be most felt in industries that use data and data-related services most intensively. Telecommunications, information and communication technology (ICT), business services, finance, and insurance are data-intensive sectors. According to the study, by comparing before and after the existing regulations, the TFP of the finance and insurance sector will decrease as follows: China (-0.34), India (-0.21), Russia (-0.43), and EU (-0.28).

The input data were inserted into a Computable General Equilibrium (CGE) model, which is frequently used in international trade measures. CGE attempts to explain the economy's functioning as a whole and estimates how an economy might react to changes in policy, technology, or other external factors by using real economic data.[96] Accordingly, the regulations in force affected the real GDP as follows: China (-0.55), India (-0.25), EU (-0.48).

---

[93] Investopedia, 'Introduction to the Solow Residual' (*Investopedia*) <https://www.investopedia.com/terms/s/solow-residual.asp> accessed 18 May 2020.
[94] Robert M Solow, 'Nobel Prize Lecture: Growth Theory and After' <https://www.nobelprize.org/prizes/economic-sciences/1987/solow/lecture/> accessed 18 May 2020.
[95] Investopedia, 'Process Value Analysis (PVA)' <https://www.investopedia.com/terms/p/process-value-analysis-pva.asp> accessed 18 May 2020.
[96] Scottish Government, 'Computable General Equilibrium Modelling: Introduction' (2016) <https://www.gov.scot/publications/cge-modelling-introduction/>.

The study also quantified the changes in the production, import, and export per sector. The most significant declines in industry output are found for communications, business, and financial services.

The break down of the changes in production, import, and export are given respectively for financial services: India: (-0.27), (-0.28), (-0.01); China: (-0.32), (-0.39), (-0.06); EU: (-0.37), (-0.06), (-0.48). As can be seen, even the exports drop as a result of the localization requirements, since the domestic production of financial services becomes less competitive against its foreign counterparts. Since the EU is more reliant on exporting services, whereas India and China focus on exporting products, the EU's decrease is more significant.

It is noteworthy to state that the Cybersecurity Law and Notice on "Urging Banking Financial Institutions to Strengthen the Protection of Personal Financial Information" of China, and The Reserve Bank of India's localization requirements, were introduced after this study, and the effects of these regulations might have an increasing impact to the numbers mentioned above. Despite that GDPR was also enacted after this paper, the draft GDPR was evaluated as part of EU legislation.

4.1.1.2. European Centre for International Political Economy Report[97]

The study conducted by the European Centre for International Political Economy aims to quantify the impact of data localization requirements and related measures in selected jurisdictions. The study uses GTAP 8 as a measurement, a CGE model, and relies on the trade data between 2004-2007 and extrapolated to 2014. The most recent model setting accounts for inter-sectoral linkages between 129 regions while capturing inter-regional trade flows of 57 commodities by analyzing the data of

[97]Matthias Bauer and others, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (2014) 32 ECIPE occasional paper <https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf>.

GDP, total population, labor force, total factor productivity, and capital endowment[98].

The paper argues that,

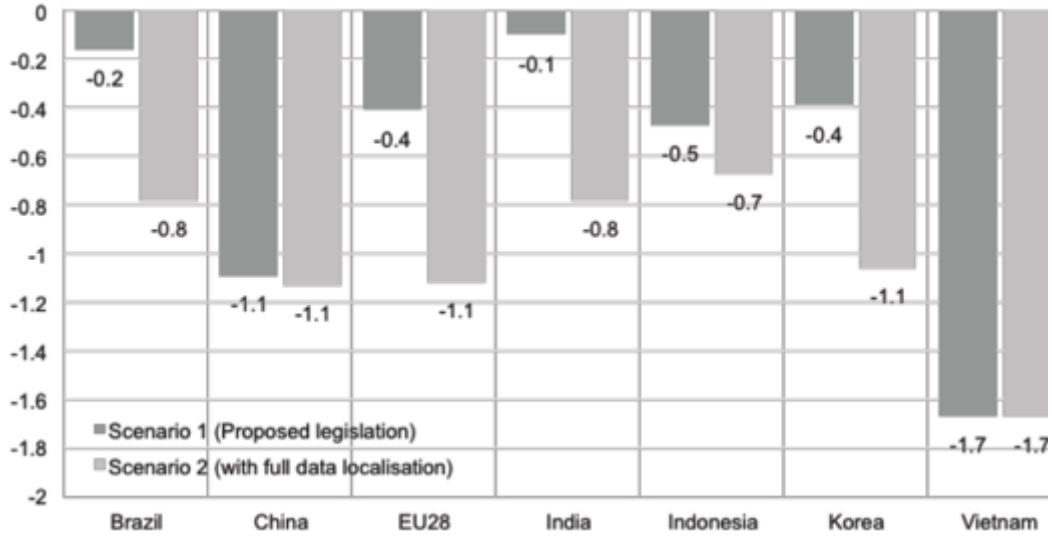
- Data localization regulations result in domestic productivity losses for various sectors, primarily for those that rely on data as input. For example, financial services is a data-intensive sector having 5-7% inputs of data related. The costs for establishing domestic data servers and the administrative burden would increase the price of products and result in TFP losses[99].
- Secondly, the requirement of installing or using data centers inside the country will decrease the investment both by domestic and foreign entities. Furthermore, the return on investments will also reduce due to the R&D expenditure[100].

The paper reviewed the current localization legislations of the selected countries by comparing them with a scenario where there is full localization.

China's GDP is estimated to decrease by -1.1% with the economy-wide full data localization. With the current privacy rules in force, the EU's GDP is decreased by (-0.4%). The full implementation of data localization rules will result in a significant decrease of (-1.1%). India's GDP is affected by (-0.1%), and the full implementation will result (-0.8%)[101]. RBI's local processing rules were not in force while these estimates were made.

[98] ibid 14.
[99] ibid 5.
[100] ibid 6.
[101] ibid.

Figure 4. 1 GTAP Simulations on Gross Domestic Product (GDP) for Selected Countries



Source: European Centre for International Political Economy Report

The full implementation of data localization rules also lowers the estimates of the International Monetary Fund (IMF) predictions. Accordingly, the IMF estimated that the GDP of China, India, and the EU would be respectively (7.7%), (4.4%), and (-0.5%) in 2014 and would have to adjust the prediction to (6.5%), (3.6%), and (-1.6%), respectively in a full localization scenario[102].

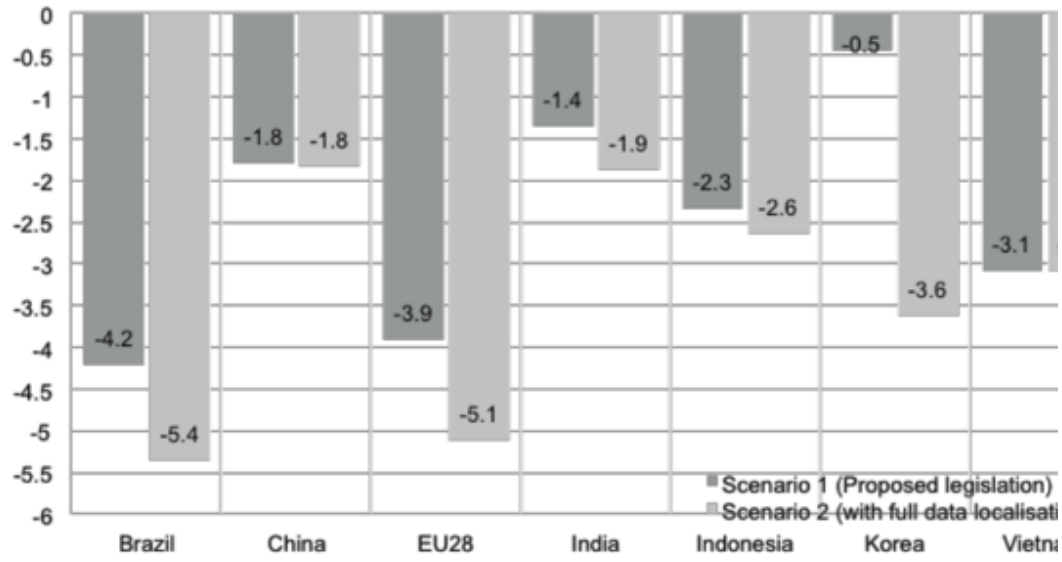
By keeping the EU's current privacy regulations, the IMF predicts that the EU will grow (0.7%) in 2015 and (2.2%) in 2016[103]. The full implementation of data localization rules would require them to amend the predictions as (-1.5%) in 2015 and (-1.1%) in 2016[104].

The current legislation will also decrease the investment, and the full localization would make it even worse. The EU's privacy rules reduce the investment by (-3.9%), whereas the partial localization in India decreases the investment by (-1.4%). China's full localization affects the investment by (-1.8%). The complete

[102] ibid 7.
[103] Euro Area real GDP growth in 2014, 2015 and 2016 were 1.4%, 2.1% and 1.9% respectively."
[104] Bauer and others (n 97) 8.

localization scenario would cost a reduction of (-5.1%) and (-1.9%) to the EU and India, respectively[105].

Figure 4. 2 GTAP Simulations on Investments for Selected Countries



Source: "European Centre for International Political Economy Report"

Besides the decrease in GDP and the investment loss, the study also looked at the welfare costs. The total welfare costs of the EU with the current legislation is $80 billion, China is $61.6 billion, and India is $3.1 billion. The full implementation would cost $193 billion to the EU and $ 14.5 billion to India. On a per-worker basis, the welfare costs are $80.7 for China, $333.9 for EU, and $6.7 for India. The costs of the full implementation would be $805.6 for a European worker and $31.5 for an Indian worker[106]. The impact would decrease 11% of the monthly salary of an Indian worker[107].

[105] ibid.
[106] ibid 9.
[107] ibid 10.

Table 4. 1 Welfare Effects from Data Localization and Privacy Barriers in Current $

	Brazil	China	EU28	India	Indonesia	Korea	Vietnam
Scenario 1	-4.7 bn.	-61.6 bn.	-80 bn.	-3.1 bn.	-2.7 bn.	-5.3 bn.	-1.5 bn.
Scenario 2	-15 bn.	-63.8 bn.	-193 bn.	-14.5 bn.	-3.7 bn.	-15.9 bn.	-1.5 bn.
Scenario 1 (per worker)	-48.9	-80.7	-333.9	-6.7	-24.9	-218.6	-31.5
Scenario 2 (per worker)	-156.1	-83.6	-805.6	-31.5	-34.1	-655.7	-31.5

Source: "European Centre for International Political Economy Report"

Overall, the report concludes that the selected countries' GDP, investment, and welfare will be affected by the localization rules. EU will be more affected since its economy is more data-driven.

4.1.1.3. US Chamber of Commerce Report[108]

This study aims to quantify the economic impact of full liberalization of ICT services by applying the expenditure approach. The general equilibrium model was not used due to the lack of data[109].

According to the study, the liberalization of cross-border ICT services would contribute to cost savings and benefit IT service vendors. Furthermore, the study indicates that new businesses and jobs will be created. Consequently, it was found that global liberalization can potentially support the GDP growth of the countries. The liberalization of the ICT services would add $7.15 billion to Turkey and $275.57 billion to the EU[110].

[108] U.S. Chamber of Commerce Internation Affairs, 'Globally Connected, Locally Delivered: The Economic Impact of Cross-Border ICT Services' (2016).
[109] ibid 20.
[110] ibid 16.

Table 4. 2 Estimated Contribution to the GDP (in $ billion)

	EU	Japan	South Korea	Brazil	Turkey	Indonesia	Vietnam	Nigeria	World
Short-Run	91.98	28.43	8.33	9.16	1.92	14.24	1.78	7.99	430.11
Medium-Run	184.35	56.19	20.76	17.37	4.60	22.05	2.64	15.74	1,075.27
Long-Run	275.57	83.64	33.01	25.44	7.15	29.38	3.46	23.43	1,720.43

Source: US Chamber of Commerce Report

4.1.2 Foreign direct investment (FDI)

We can evaluate the impact of data localization rules regarding FDI by dividing it into two parts. a) Data Center Investment, b) Service/Product Investment.

Requiring the financial institutions to install or use locally installed data centers would increase the domestic data center investment since the demand will increase, and the land and construction costs would require the entities to bring a substantial capital investment into the country. However, the land and construction expenses are one time investments. Apple paid $1.7 million for the land in North Caroline, which is a one-time expense.

Some companies also see the localization requirement as digital mercantilism, similar to the tariffs to protect local manufacturing operations. According to the survey among American companies, 23% of small and medium-sized enterprises (SMEs) and 19% of large firms in finance see localization requirements as a substantial trade barrier[111].

Countries are devising relationships that forbids localization requirements. For example, the EU prohibits member states from enacting data localization rules and labels such regulations as a threat to the economy. Likewise, the signatory countries of CPTPP and USCMA undertakes to allow financial institutions to transfer

[111] U.S. International Trade Comission, 'Digital Trade in the U.S. and Global Economies - Part 2' 331, 23 <http://www.usitc.gov/publications/332/pub4485.pdf>.

information into and out of their countries for data processing – subject to certain conditions.[112]

The companies domiciled in the countries mentioned above will want to invest in a more business-friendly environment with legal backing. Thus, the companies that see the localization requirements as a substantial trade barrier, or contradict their policy for many reasons, might decide to invest further in a different country or exit the country. Thus, implementing localization rules might create an adverse effect in companies choosing not to invest or exiting the market. For example, as explained below, PayPal ceased its Turkish operation due to localization rules.

As stated in the reports mentioned above, the investment will decrease significantly, and that the increase in domestic data center investment will not help recover the losses. The real contribution to the economy will not be through one time expenses such as construction and land expenses, but through the value created from data-driven technologies/services.

4.1.3 New job creation

Some argue that the localization rules will encourage building data centers and create new skilled jobs. Accordingly, they point out that Facebook's data center in Sweden contributed to the local and national economy[113]. On the contrary, the report of the US Chamber of Commerce claims that the liberalization of the Information and Communication Technology (ICT) services will create jobs. Accordingly, the job cuts will likely be absorbed by the IT service vendors or new businesses. The report indicates that the global liberalization of ICT services would lead to a net job

[112] Australian Government Department of Foreign Affairs (n 22).
[113] Shamel Azmeh and Christopher Foster, 'The TPP and the Digital Trade Agenda: Digital Industrial Policy and Silicon Valley's Influence on New Trade Agreements' (2016) 44 London School of Economics 35, 26 <http://www.lse.ac.uk/internationalDevelopment/home.aspx>.

creation of 23.400 jobs in Turkey among 23.04 million jobs around the selected jurisdictions in the long run[114].

Table 4. 3 Estimated Net Job Creation ('000 jobs)

	EU	Japan	South Korea	Brazil	Turkey	Indonesia	Vietnam	Nigeria	World
Short-Run	759.8	143.2	127.1	27.1	31.6	1,012.7	51.4	336.2	5,759.4
Medium-Run	1,823.0	337.3	316.5	52.8	77.5	1,377.8	62.2	796.5	14,398.5
Long-Run	2,886.2	531.4	505.8	78.4	123.4	1,742.9	72.9	1,256.8	23,037.7

Source: US Chamber of Commerce Report

Besides, the rise in data centers may not translate into a significant increase in employment since "data centers are usually highly automated, and allows a small number of works to operate a large facility."[115] Reports suggest that "data centers may only employ an average of five to thirty people." [116] These reports are in line with reality. While Apple provides 50 full-time jobs in its $ 1 billion worth data center in North Caroline, Google employs around 100 jobs, including contractors at its $ 600 million worth data center.[117] Likewise, Turkey's biggest data center belonging to Turkcell employs around 50 full-time workers. Microsoft's data center in Washington employs 50 full-time employees to manage the center.[118]

Thus, a new data center can bring a substantial capital investment into the country but create a much smaller number of jobs than a factory of a similar size. For

[114] U.S. Chamber of Commerce Internation Affairs (n 108) 15.
[115] Quentin Hardy, 'Cloud Computing Brings Sprawling Centers, but Few Jobs, to Small Towns - The New York Times' (2016) <https://www.nytimes.com/2016/08/27/technology/cloud-computing-brings-sprawling-centers-but-few-jobs-to-small-towns.html> accessed 20 July 2019.
[116] Alison DeNisco Rayome, 'Why Data Centers Fail to Bring New Jobs to Small Towns - TechRepublic' (2016) <https://www.techrepublic.com/article/why-data-centers-fail-to-bring-new-jobs-to-small-towns/> accessed 20 July 2019.
[117] Michael S Rosenwald, 'Cloud Centers Bring High-Tech Flash but Not Many Jobs to Beaten-down Towns - The Washington Post' (2011) <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> accessed 3 May 2020.
[118] Rich Miller, 'The Economics of Data Center Staffing | Data Center Knowledge' <https://www.datacenterknowledge.com/archives/2008/01/18/the-economics-of-data-center-staffing> accessed 4 May 2020.

example, Volkswagen's planned investment for a $ 1.4 billion worth car production facility in Turkey is expected to create 5.000 jobs[119].

4.1.4. Energy market and environmental effect

Energy consumption is one of the hottest topics discussed around climate change. According to the report[120] of the International Energy Agency (IEA), data centers consumed about 1% (200 TWh) of global electricity use in 2018, and it forecasts that this would stay flat until 2021. However, Vidal suggests that, with the usage of the new developing technologies, the total consumption of the data centers could reach 20% by 2025[121].

The IEA report breaks down the total consumption into three types of data centers, i.e., hyperscale cloud, non-hyperscale cloud, and traditional. Hyperscale data centers proportionally consume much less energy than smaller data centers due to the increasingly efficient IT hardware. The number of hyperscale data centers globally is expected to reach 628 in 2021 then 259 in 2015. Between the same period, the share of all data center traffic will rise from 34% to 55%.

The availability and cost of electrical power infrastructure are deemed as one of the most important selection criteria to determine the location of the data center[122]. Due to environmental effects, the most significant companies are pledging to cover all of the energy consumption from renewable energy, which adds a more precise criterion. In 2018, Google and Apple purchased or generated 10 TWh and 1.3 TWh, respectively, from wind and solar energy enough to match all of their data center

[119] Christoph Rauwald, Tugce Ozsoy and Ercan Ersoy, 'Volkswagen Turkey Unit Paves Way for $1.4 Billion Plant - Bloomberg' <https://www.bloomberg.com/news/articles/2019-10-02/volkswagen-establishes-unit-to-manufacture-cars-in-turkey> accessed 3 May 2020.
[120] George Kamiya and Kvarnström Oskar, 'Data Centres and Energy – from Global Headlines to Local Headaches?' (2019) <https://www.iea.org/commentaries/data-centres-and-energy-from-global-headlines-to-local-headaches>.
[121] John Vidal, '"Tsunami of Data" Could Consume One Fifth of Global Electricity by 2025' *Climate Home News* (2017) <https://www.climatechangenews.com/2017/12/11/tsunami-data-consume-one-fifth-global-electricity-2025/>.
[122] Intel, 'Selecting a Data Center Site: Intel's Approach' (2014) 11.

energy consumption. Facebook covered 75% of its 3.2 TWh energy consumption from renewable energy[123].

Thus, the costs of energy and the renewable energy infrastructure are essential when deciding on the location. EIRGRID forecasts that demand from data centers could account for 29% of all demand in Ireland by 2028[124], whereas Danish Energy Agency estimates that data centers might consume 15% of total energy consumption in Denmark in 2030[125]. Both Denmark and Ireland plan to cover half of their total consumption from wind and solar energy.

Turkey is an energy exporter that provides most of its energy from fossil fuels and is vulnerable to fluctuating prices. The lack of renewable energy might prevent the hyper-scale data center providers from investing in Turkey. The dependence on fossil fuels might harm the environment, and the increasing demand for energy for data centers may cause further stress on an already depleted energy sector[126].

4.2. IMPACT ON FINANCIAL INDUSTRY

This section will focus on the effect of localization rules on the financial industry by examining innovation, security, open banking, mobile money remittances, and e-commerce.

4.2.1. Costs of localizing IT infrastructure

According to a study held by *Leviathan,* which looks at the impact of data localization rules on the businesses, by calculating the cost difference on a per-hour, per-server level, it was determined that the localization rules would increase the

[123] Kamiya and Oskar (n 120).
[124] EIRGRID, 'All-Island Generation Capacity Statement - 2019-2028' (2019) 11.
[125] Danish Energy Agency, 'Denmark's Energy and Climate Outlook 2019' (2019) 24.
[126] Basu, Hickok and Chawla (n 80) 26.

costs for the companies. The study focused on public "Infrastructure as a Service" (IaaS) cloud computing providers and found only "seven cloud providers globally met the selected criteria."[127] The servers of these providers are located in twelve countries.[128] The researchers found that possible data localization requirement at some of these countries would require their companies to pay around 30-60% more for their computing needs than if they could go outside the country's borders.[129]

The companies subjected to localization requirements and are not in the selected twelve countries would bear much higher costs for using local data centers. Either they would have to install data centers by allocating capital investment in hardware and incurring its maintenance costs, or they would have to use the local providers with a higher price and less tools.

Besides the increasing costs for the companies, the cost-saving impact for the countries is also significant. According to the US Chamber of Commerce report, Turkey might save $ 1.75 billion by liberalizing the ICT services[130]. (Table 4.4)

The increasing costs suggest that the barriers to cross-border data flows make firms less competitive since a company will be forced to spend more than necessary on IT services.

Table 4. 4 Estimated Cost Saving Impact (in $ billion)

EU	Japan	South Korea	Brazil	Turkey	Indonesia	Vietnam	Nigeria
68.17	17.84	7.42	5.62	1.75	3.04	0.22	1.15

Source: US Chamber of Commerce Report

[127] Amazon Web Services, DigitalOcean, Google Compute Engine, HP Helion Public Cloud, Linode, Microsoft Azure and Rackspace Cloud Servers

[128] United States, Brasil, Germany, Netherlands, Belgium, United Kingdom, Japan, Australia, Hong Kong, Taiwan, Singapore, Ireland." "Brendan O'Conner, 'Quantifying the Cost - Interactive Data Visualization' <http://cloudsecurity.leviathansecurity.com/> accessed 9 May 2020.

[129] Brendan O'Connor, 'Leviathan Security Group - Quantifying the Cost of Forced Localization' (2015) <https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf>.

[130] U.S. Chamber of Commerce Internation Affairs (n 108) 13.

4.2.2. Innovation

For an extended period, most individuals only had a bank account on a physical bank and could only carry out transactions by visiting the branches of the banks. The branch numbers was one of the main measures in determining the size of a bank. Nowadays, there are banks without physical branches, and the business model is drastically changing. Many physical banks transferred their investment focus to online services rather than physical presence. Today, most individuals can manage their bank accounts and handle all kinds of banking activities instantly with a mobile device online, and the physical presence of branches became a burden rather than a growth strategy.

Innovation in payment services has been based on the traditional card systems, and besides the banks, massive credit card companies such as Visa, Mastercard, and American express merged. The banks were also the leaders of this ecosystem by issuing their own cards with credit card companies' collaboration. Today, there are many innovative companies with different business models that challenge the dominance of traditional financial institutions.

Innovation and growth are increasingly driven by how firms collect, transfer, analyze, and act on data. Organizations use data to create better insights, which, in turn, lead to innovation. Businesses use data to enhance research and development, develop new products and services, create new production or delivery processes, improve marketing, and establish new organizational and management approaches. Barriers to data flows also mean delays and higher costs in developing new and innovative products, as companies may be unable to use their preferred partners, technology, and products/services.

The Committee led by Justice Srikrishna points out that localization measurements may help create digital industry and digital infrastructure, benefitting AI and other emerging technologies by providing big data from the servers installed locally. Accordingly, they argue that the data can be anonymized and shared with start-ups

or other businesses.[131] They also highlight the reports that forecast the weight of AI to the economic growth. According to Accenture, AI will contribute to both Chinese[132] and India's economy with 1.6% and 1.3%[133], respectively, by 2035.

Most of the technologies of the 4th Industrial Revolution are indeed exceptionally reliant on accessing and processing data. However, to realize the potential of such data-intensive technologies or to fully harness the power and efficiency of them, the technologies, such as AI, IoT, blockchain, and the cloud, are important as the data itself. Most of these technologies require the movement of data across country borders.

The local data may somehow fuel the development of AI and emerging technologies. However, this also possible while there is access to the data hosted abroad and an effective data sharing mechanism. On the contrary, preventing data from being hosted outside of the country might prevent companies from using the services and the technologies that drive innovation.

4.2.3. Security

The new technologies are the main driver for economic growth, while the threats increase subsequently. The prevalence of AI, IoT, blockchain, and 5G requires more advanced cybersecurity solutions to defend against cyberattacks. Security must escort innovation.

Identity Theft Resource Center reported that 163 million records were exposed due to 1.272 breaches as of November 2019. The banking and healthcare industry, with the most sensitive data, experienced the highest percentage of breaches. According

[131] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 'A Free and Fair Digital Economy Protecting Privacy , Empowering Indians' 92.
[132] Accenture, 'HOW ARTIFICIAL INTELLIGENCE CAN DRIVE CHINA'S GROWTH' <https://www.accenture.com/cn-en/insight-artificial-intelligence-china>.
[133] Accenture, 'REWIRE FOR GROWTH: Accelerating India's Economic Growth with Artificial Intelleginc' (*Accenture*, 2017) <https://www.accenture.com/_acnmedia/PDF-68/Accenture-ReWire-For-Growth-POV-19-12-Final.pdf>.

to the IBM Security and Ponemon Institute study, the average costs of a stolen or lost record corresponded to $150 in 2019[134].

4.2.3.1. Data security

Multinational companies mostly adopt a diversification approach to ensure data security across a geographically distributed network, uses complicated cybersecurity products, and pour millions to ensure security. Data localization rules create a barrier towards reaching the ultimate level of security provided by these companies.

Firstly, establishing an up-to-date global and secure IT system would cost a lot for the banks and fintechs. Even if the entities afford the costs, considering that security is not the core business of financial institutions, they might not act swiftly towards such threats or attacks. The Cisco survey shows that 25% of the respondents (CTO) indicated that they do not know what to do after a security breach[135]. Security companies spend billions of dollars and educate employees about the threats. For instance, Microsoft's R&D budget is $19.3 billion for 2020, and around €2 billion of the budget is allocated for cybersecurity.

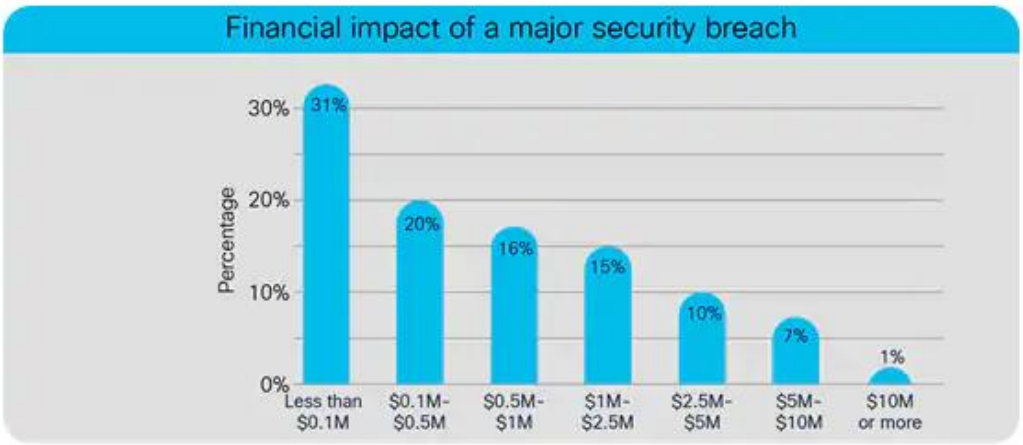
Secondly, the cyber threats against financial institutions become much more intelligent, targeted, and intentional. Data localization, as a conventional method, is far from preventing such threats. Thus, the regulatory bodies must enable and support the financial institutions to use real-time intelligence security products. Data localization prevents the use of such products and makes the entities vulnerable against such attacks. For example, the cyberattack back in 2016[136] against Turkish banks, including Akbank,[137]showed that the localization is not

[134] Cisco, 'Cisco Annual Internet Report' (2020) 21.
[135] ibid 31.
[136] Reuters, 'Turkey's Akbank Faces $4 Million Hit from Attempted Cyber Heist' (2016) <https://www.reuters.com/article/us-akbank-cyber-idUSKBN1450MC>.
[137] Akbank keeps all their data in its own data centers within Turkey. They are prevented to use any global security products which are based on public cloud or on a foreing server in line with the Banking Law.

enough to prevent such threats, and equally intelligent and secure products must defy such attacks.

Given the extent of the monetary and brand damage associated with data breaches, cybersecurity is treated as a business risk rather than merely an IT issue. The damage caused by such a breach might damage the entity's reputation, and the realization of the damage could only be quantified after the attack. According to the IBM Security and Ponemon Institute study, the average costs of a stolen or lost record corresponded to $150 in 2019[138]. According to a survey held among 2.386 Chief Information Security Officers (CISO) 33% of the respondents stated that security breaches created more than $1 million damage.[139]

Figure 4. 3 Financial impact of a Major Security Breach



Source: Anticipating the unknowns: Chief Information Security Officer (CISO) Benchmark Study, Cisco, March 2019

The security and compliance standards of data should be more important than the physical location of data. The extra costs of localization might shift the focus from the security aspects and decrease investments, causing material damages. Thus, data localization requirements in the name of cybersecurity are often misguided policies.[140]

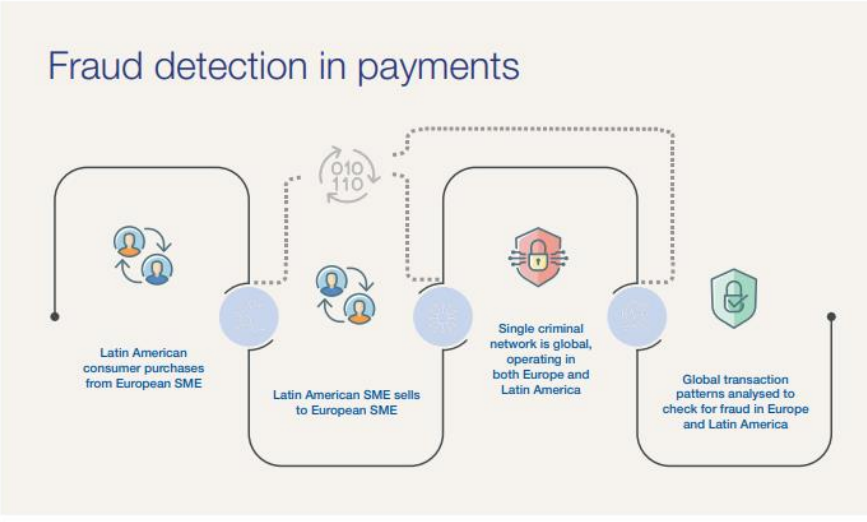
[138] Cisco (n 134) 21.
[139] ibid 30.
[140] World Economic Forum (n 36) 13.

4.2.3.2. Money laundering and financing of terrorism

Data localization requirements can compromise the ability to detect fraud, money laundering, and terrorism financing activities globally. By limiting the flow of data across borders, the process of detecting suspicious activities becomes more complicated.

For instance, the safe and secure provision of remittances relies on strict anti-money laundering (AML) and combating the financing of terrorism (CFT) processes, which typically involve sharing data across borders. The data localization requirements may directly conflict with both regulatory frameworks, and this can also lead to increased risks of money laundering and the financing of terrorism[141].

Figure 4. 4 Fraud Detection in Payments[142]



Source: World Economic Forum

[141] Claire Scharwatt, 'The Impact of Data Localisation Requirements on the Growth of Mobile Money-Enabled Remittances' (2019) 5.
[142] Abdelhamid Mamdouh and others, 'Exploring International Data Flow Governance Platform for Shaping the Future of Trade and Global Economic Interdependence' (2019) 13 <http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf>.

The recently published Fincen documents show the urgency of how countries must act to tackle money laundering and terrorism activities[143]. This requires collaboration between countries and financial institutions. For example, there is an international agreement in force requiring countries to share financial information to prevent tax evasion. Likewise, it is impossible to tackle money laundering and terrorism activities without sharing data, using cloud-based intelligent products (Figure 4.4), and devising effective mechanisms[144].

4.2.4. Open Banking

As financial institutions are becoming digital in a more and more globalized world, the regulation perspective is also changing. Regulative efforts, such as PSD2, are implemented to support fintechs. These regulative efforts aim to provide a safe, secure and efficient system where banks can share information with fintechs. This data sharing process, aimed to increase the innovation and competition in the industry, with nonbanks, is called Open Banking[145].

Notably, banks have traditionally viewed the custody of their clients' data as a responsibility, more of a gatekeeper role than an asset to be commercialized[146]. However, the open banking provisions empowers account holders to let the banks to share data with nonbanks, removing the banks' role as a gatekeeper and forcing them to share their power with other players. This process aims to commercialize the data and benefit the customers.

---

[143] BuzzFeed News, '8 Things You Need To Know About The Dark Side Of The World's Biggest Banks, As Revealed In The FinCEN Files' (2020) <https://www.buzzfeednews.com/article/jasonleopold/fincen-files-8-big-takeaways> accessed 7 October 2020.

[144] CONVENTION ON MUTUAL ADMINISTRATIVE ASSISTANCE IN TAX MATTERS 1988."

[145]Laura Brodsky and Liz Oakes, 'Data Sharing and Open Banking' (2017)."*Open banking can be defined as a collaborative model in which banking data is shared through APIs between two or more unaffiliated parties to deliver enhanced capabilities to the marketplace*"

[146]ibid 3.

These legal requirements of sharing customer data force the fintechs and banks to devise a complicated relationship by competing and collaborating at the same time. The new type of relationship that exists in the financial industry could be defined as coopetition[147].

According to McKinsey's survey among the executives of the European Banks, 55% of the respondents think that fintech innovators and small and medium-size banks are better placed to move fast and disrupt the payments market. The 25% expects that large banks will benefit most from such rules[148].

However, the global trend suggests that a substantial portion of revenues will change hands. Mckinsey estimates that a service provider offering Account-to-Account solutions could generate €50 million to €100 million of revenues that are currently generated by banks[149]. The European banks are positioning themselves by cutting deals with new service providers by offering their API and technology and re-building their ecosystem in line with the new trend. 40% of the executives stated that they have already selected vendors/partners to render their services[150].

As a result of the data-driven ecosystem, many players such as Square, PayPal, ApplePay, GooglePay, Xero, Intuit, Finicity[151], Tala, Klarna, Fidor, Klarna, N26, and AliPay already thrived in their region and globally.

The European banks and fintechs uses cloud to re-invent their business, cut unnecessary costs, and focus on the main business. As explained in Section III and despite their huge budget and sources, 67% of the banks in Europe are already using cloud services, and there is no restriction preventing them from using it. Fintechs do not have the means and sources to develop big data centers, pour money into the

[147]Investopedia, 'Coopetition' <https://www.investopedia.com/terms/c/coopetition.asp>."Coopetition is the act of cooperation between competing companies; businesses that engage in both competition and cooperation are said to be in coopetition. Certain businesses gain an advantage by using a judicious mixture of cooperation with suppliers, customers, and firms producing complementary or related products.
[148]Alessio Botta and others, 'PSD2 : Taking Advantage of Open- Banking Disruption' (2018) 7.
[149]ibid 5.
[150]ibid 8.
[151]Finicity is a cloud-based platform that offers transaction management, credit decisioning and data aggregation solutions for the financial sector.

infrastructure and maintenance. Their existence is mostly dependent on public cloud services. For instance, The CEO of Fidor attributed the company's success to cloud computing, stating that they could not create such an innovative service without having to invest in costly infrastructure. Likewise, Mike Laven, CEO of Currency Cloud, which formed a cloud-based partnership with Fidor, stated that they had built the foreign exchange payment system in two weeks, whereas it would take 18 months if Fidor were to build it on its own. He also expressed that on the contrary view that cloud computing and banking are not a good match, cloud computing services "can provide high-security, conform to regulations, and offer best practice in encryption, because of security concerns."[152]

Forcing the fintechs to install or use locally installed data centers will put an extra burden from a cost and time perspective, deprive them of using the SaaS[153], and prevent them from forming cloud-based partnerships. Fintechs without cloud solutions will not have the tools to compete with traditional financial institutions and well-established banks and will stay behind the competition. The expert committee led by Justice Srikrishna, which is mainly supportive of localization rules, acknowledges that such rules would lead the SMEs to pay a higher amount for installing or renting such local infrastructure, leading to monopolization[154]. To conclude, the localization rules would undermine the efforts in opening the financial industry to innovation and competition.

4.2.5. Money Remittances

Cross-border remittance transfers are growing significantly due to the increasing volume of international trade and immigration flows. US alone hosts 46.1 million international migrants, while the top emigrated countries are India, Mexico, Russia,

[152] Jane Bird, 'Cloud Is Silver Lining for German Online Bank Fidor' *Financial Times* <https://www.ft.com/content/4eea4798-81c6-11e3-87d5-00144feab7de>.
[153] SaaS: Software as a service; software solutions that reside in the cloud but, due to high-speed connectivity, can be used in real time as if they resided locally.
[154] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (n 131) 94.

and China. Likewise, in current US dollar terms, the top remittance recipient countries are projected to be India ($82.2b), China ($70.3b), Mexico ($38.7b), the Philippines ($35.1b), and Egypt ($26.4b). While, in the GDP percentage terms, Khrigizstan (29.6%), Tajikistan (29.7%), West Bank, and Gaza (17.6%) are among the leading recipient countries.

Over the past few years, a number of mobile money services have expanded to facilitate cross-border transfers. As of 2019, there are 184 channels where mobile money can be used to send and/or receive international remittances. This enables providers to significantly drive down remittance costs, positioning mobile money as a critical tool to achieve Sustainable Development Goal target 10.c.[155]

However, according to the World Bank's Remittance Prices Worldwide Database, the average cost of sending $200 to LMICs was 6.8 percent in the second quarter of 2019 and 6.9 for the MENA region. This is still more than double the Sustainable Development Goal (SDG) target of 3 percent by 2030 (SDG target 10.c), which was settled as one of the objects in decreasing the inequality within and among the countries.

Figure 4. 5 How Much Does It Cost to Send $200?

Source: Remittance Price Worldwide database, World Bank

[155] Scharwatt (n 141) 3.

World Bank reported that low and middle-income countries are expected to receive $597 billion by 2021[156], requiring $40.596 billion in costs according to the average cost of 6.8%, assuming that each transaction is 200 dollars. However, according to the Sustainable Development Goal (SDG) target, the cost must have been $17.910 billion. The gap between the reality and target is $22.686 billion.

Many projects are launched and are in progress, aiming to provide a more secure, cheap, and fast way to transfer funds worldwide. These approaches benefit AI, Blockchain, and IoT technologies, which are not suitable for data localization practices.

For example, JP Morgan Chase launched Interbank Information Network (IIN) chain with the participation of 300+ banks. The system aims for near-instant resolution of issues like removing the rejection possibility of the payments that may come days later because of an error in an account number, address, or other aspects of the transaction by using blockchain technology[157].

Likewise, SWIFT is also working on improving its cross border transaction system with a blockchain-based system. Accordingly, the banks within the system will use the application programming interface to access each other's data to check the information's validity. API will be under the blockchain-based system, and the information will be shared on a mutually distributed ledger hosted on the cloud that can be accessed and edited by all participants in real-time[158]. Swift is also getting ready to implement ISO 22022 in 2021 for cross-border transfers, which will bring many advantages, including eliminating the need for translation and transformation

[156] World Bank, 'Data Release: Remittances to Low- and Middle-Income Countries on Track to Reach $551 Billion in 2019 and $597 Billion by 2021' (2019) <https://blogs.worldbank.org/peoplemove/data-release-remittances-low-and-middle-income-countries-track-reach-551-billion-2019>.
[157] JP Morgan, 'J.P. Morgan Interbank Information Network® Grows to 300+ Banks' (2019) <https://www.jpmorgan.com/country/US/EN/detail/1320575182345>.
[158] Laura Noonan, 'Swift Takes on Fintechs with New Payment System' (2018) <https://www.ft.com/content/05d41660-f7c8-11e8-af46-2022a0b02a6c>.

between internal and external market systems by creating a single global language[159].

Many global companies are in a race to provide a more secure, fast, and cheap way to transfer remittances. Ripple, PayPal, and Transferwise decreased the costs of sending remittances abroad significantly. The exchange of cryptocurrencies also offers a bright future. The SDG target of 3% could only be achieved by decreasing the costs and encouraging the use of new technologies.

4.2.6. E-Commerce & Payment Methods

In this section, we will review the global e-commerce market, the role of payment services, and their importance regarding customer choice. The data localization requirement of e-commerce platforms will not be discussed in this section and will solely focus on the payment methods.

4.2.6.1. E-Commerce

With the digitization of trade, e-commerce is one of the leading factors contributing to the world economy. United Nations Conference on Trade and Development (UNCTAD) published a report of 2018 based on the data provided by the countries[160]. According to the report, e-commerce sales reached $25.6 trillion globally in 2018, including B2B ($21 trillion) and B2C ($4.4 trillion)[161].

[159] SULABH AGARWAL, 'WHY ISO 20022 IS A SEISMIC SHIFT FOR PAYMENTS' (*Accenture*, 2020) <https://bankingblog.accenture.com/iso20022-seismic-shift-payments> accessed 22 November 2020.
[160] UNCTAD, 'UNCTAD Estimates of Global E-Commerce 2018' (2020) <https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d12_en.pdf>.
[161] ibid 1.

The importance of e-commerce is immense. The statics show that the share of total e-commerce sales to GDP corresponds to 66% in Japan, 29% in France, and 84% in Korea[162].

Table 4. 5 Total e-commerce sales to GDP

Rank	Economy	Total e-commerce sales ($ billion)	Share of total e-commerce sales in GDP (%)	B2B e-commerce sales ($ billion)	Share of B2B e-commerce sales in total e-commerce (%)	B2C e-commerce sales ($ billion)
1	United States	8,640	42	*7,542*	87	*1,098*
2	Japan	3,280	66	3,117	95	163
3	China	2,304	17	943	41	1,361
4	Korea (Rep.)	*1,364*	84	*1,263*	93	102
5	United Kingdom	918	32	652	71	266
6	France	807	29	687	85	121
7	Germany	722	18	*620*	86	101
8	Italy	*394*	19	*362*	92	*32*
9	Australia	348	24	326	94	21
10	Spain	333	23	261	78	72
	10 above	**19,110**	**35**	**15,772**	**83**	**3,338**
	World	***25,648***	**30**	***21,258***		**4,390**

Source: UNCTAD, based on national sources

B2C sales also contributed to the economy significantly. The numbers show that the share of B2C e-commerce sales to GDP corresponds to 9.8% in United Kingdom, 10.4% in Hong Kong, China, and 10% in mainland China[163].

[162] ibid 2.
[163] ibid 3.

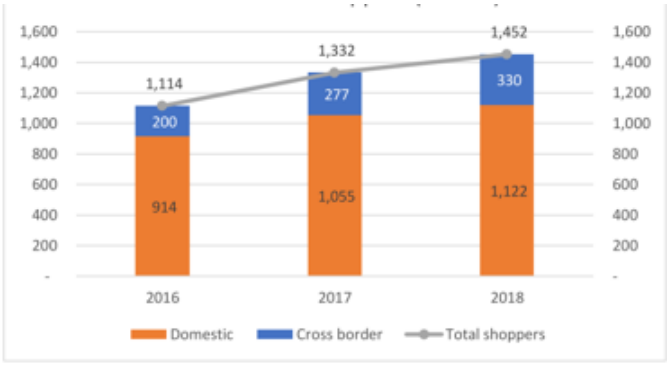
Table 4. 6 B2C e-commerce sales to GDP

Rank	Economy	B2C e-commerce sales ($ billion)	Share of B2C e-commerce sales in GDP (%)	Online shoppers (million)	Online shoppers (% of Internet users)
1	China	1,361	10.0	610	73
2	United States	1,091	5.3	189	80
3	United Kingdom	266	9.3	41	87
4	Japan	163	3.3	49	49
5	France	109	3.9	36	75
6	Korea (Rep.)	102	6.3	27	60
7	Germany	101	2.6	54	82
8	Spain	72	5.1	21	62
9	Canada*	44	2.6	24	84
10	Hong Kong, China	38	10.4	2	38
11	Italy	32	1.6	18	47
12	Netherlands	28	3.1	12	84
13	Thailand	27	5.3	5	14
14	Mexico	26	2.1	24	33
15	Ireland	22	5.7	2	70
16	Australia	21	1.5	12	73
17	Russian Federation	20	1.2	30	34
18	Malaysia	19	6.0	15	53
19	India	17	0.6	27	11
20	Brazil	15	0.8	39	34
	20 above	**3,574**	**5.3**	**1,193**	**55**

Source: UNCTAD, based on national sources

The cross-border B2C e-commerce sales corresponded to $404 billion, resulting from 330 million online customers. Accordingly, the share of cross border online customers to all online shoppers rose from 20% in 2017 to 23% in 2018[164].

Figure 4. 6 Global online shoppers (million)



Source: UNCTAD, based on national sources

[164] ibid 5.

United Kingdom generated $40 billion from cross-border B2C sales, 8.2% of its merchandise exports. Germany and the United States generated $15 and $85 billion respectively from cross-border B2C sales. The total share of cross-border B2C sales in B2C e-commerce sales is 94.3% for Hong Kong, China, 15% for the United Kingdom, and 14.9% for Germany[165].

Table 4. 7 Total Share of Cross Border B2C sales in B2C E-Commerce Sales

Rank	Economy	Cross-border B2C e-commerce sales ($ billion)	Share of cross-border B2C e-commerce sales in merchandise exports (%)	Share of cross-border B2C sales in total B2C e-commerce sales (%)
1	China	100	4.0	7.3
2	United States	85	5.1	7.8
3	United Kingdom	40	8.2	15.0
4	Hong Kong, China	35	6.2	94.3
5	Japan	21	2.9	13.1
6	Germany	15	1.0	14.9
7	France	12	2.0	10.6
8	Italy	4	0.8	13.9
9	Korea (Rep.)	3	0.5	3.2
10	Netherlands	1	0.2	4.4
	Ten above	**317**	**3.2**	**9.6**
	World	**404**	**2.1**	

Source: UNCTAD estimates based on national sources,

Source: UNCTAD, based on national sources

Turkey received $12.4 billion from e-commerce in 2018[166], less than the amount of the cross-border B2C e-commerce sales of Germany ($15 billion). However, there is no data concerning Turkey's cross-border e-commerce sales to compare it with other countries.

4.2.6.2. The role of Payment Services

Payment systems are an essential part of e-commerce platforms. These platforms offer multiple payment providers so that the customers/businesses could easily purchase goods and services as they wish so. Mainly banks with the support of

[165] ibid.
[166] TÜBİSAD, 'Türkiye'de E-Ticaret 2018 Pazar Büyüklüğü' (2019) 13 <http://www.tubisad.org.tr/tr/images/pdf/tubisad_2019_e-ticaret_sunum_tr.pdf>.

payment networks such as Visa and Mastercard and global payment services such as PayPal, AliPay, and Square provide customer choice.

According to a report of KMPG, 34% of customers decide where to buy the services or goods based on the payment options that the e-commerce platform provides, whereas 57% of the customers select the goods and services with the lowest price[167].

65-79% of the customers purchase the products and services with credit cards, whereas PayPal is the second widely used method and a close second to credit cards in more developed countries[168].

Figure 4. 7 Percentage of Consumers that Use Payment Method – by Region

Source: 2017 Global Online Consumer Report, KPMG

[167] KPMG, 'The Truth about Online Consumers - 2017 Global Online Consumer Report' (2017) 29 <https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/01/the-truth-about-online-consumers.pdf>.
[168] ibid 31.

4.2.6.3. Localizing the Data of Payment Services

As can be seen above, most of the surveyed uses more than one payment method. This means that the customers are flexible concerning payment methods and might shift the payment option based on the product price or other reasons. In the meantime, the 34% customers (who choose the e-commerce platform based on the payment options) would instead select an e-commerce platform that accepts the preferred payment method rather than shifting the payment method itself. PayPal alone processes a high amount of the $404 billion cross-border e-commerce market since 32-35% of the customers use it for payment. Thus, the lack of PayPal or other global payment providers, which operates data centers abroad for processing and storing, might significantly affect e-commerce sales. The VP of Ingenico stated that one of the most important points is to offer the right payment methods to the population to enable global participation[169]. The CMO of Asendia also believes that the key challenges for e-retailers relate to "delivery and payment options."[170] The more the e-commerce platforms offer payment methods, the more the customers are likely to purchase the product/service.

65% of the customers compare the prices of the goods/services at the e-commerce platforms[171] and select the platform that offers the lowest price. According to the survey mentioned above, 57% of the customers decide where to buy the product/service based on the lowest price, and 34% of the customers think that the best price is the most important factor[172]. Thus, the product's price is one of the main drivers of the customer when making the decision. As explained in section 4.2.1., installing or using data centers within the country is likely to increase the costs of storing and processing data. Thus, the localization requirement will increase payment processing costs and increase the price of the goods and services of the e-commerce platform. For example, if the product price is lower in Germany

[169] Ecommerce Foundation, 'Global Ecommerce Report 2017' (2017) 74.
[170] ibid 85.
[171] ibid 71.
[172] ibid 58.

than in Turkey, the customer in the UK would likely purchase the product in Germany rather than the one in Turkey. This would make the Turkish e-commerce market less competitive to compare with other countries.

4.3. PAYPAL EXIT IN TURKEY

Paypal was devised as eBay's exclusive payment system until it became an independent company and reached 200 different countries/regions. The company holds a payment transmitter license in the US, a credit institution license in Luxemburg, and a stored value facility holder in Singapore. According to the 2019 annual report, PayPal has 305 million active users, including 24 million merchants, and 40.6 payment transactions were held per user[173].

PayPal, in 2015, decided to migrate its infrastructure to the public cloud and chose Google as its service provider. According to PayPal's CTO, they have migrated 15% of their infrastructure to Google Cloud as of 2018 and chose Public Cloud for the following reasons: scale, flexibility, regulation adoption, efficiency, and innovation. The CTO acknowledged that some countries require local processing and storing, and they try to comply with the local requirements. However, he also stated that they could not install data centers for all the jurisdictions, which is why they have partnered with Google to make their services accessible to their customers around the globe.[174] PayPal's migration to Public Cloud is increasing[175], and they see the public cloud and the services in it as indispensable to their business.

[173] PayPal, 'PayPal 2019 Annual Report' (2020) <https://investor.paypal-corp.com/static-files/6b4a31d7-9941-464d-846d-3859fd7058dc>.
[174] 'PayPal Partners with Google Cloud' (2018) <https://www.youtube.com/watch?time_continue=30&v=9jJ6xLOSS3c&feature=emb_logo> accessed 2 May 2020.
[175] David Penn, 'PayPal Takes to the Google Cloud - Finovate' <https://finovate.com/paypal-takes-to-the-google-cloud/> accessed 1 May 2020.

The cloud policy of PayPal can be viewed at the following words of the CTO "public cloud is no longer a matter of if it's a matter of when."[176]

PayPal started to enable its customers in Turkey to use its services in 2004. However, its license application was rejected by the BDDK in 2016 for not installing their information systems and back-ups locally[177]. As mentioned in section 3.1, all the infrastructure of the payment services and electronic money institutions in Turkey must be installed locally. However, looking into PayPal Turkey's Privacy Policy valid until 1 June 2015, it can be seen that the storing and processing of data were held on their facilities located in North America, Asia, Europe, and anywhere in the world, in which Turkey is not among them[178]. Although PayPal did not state it openly, the strategy shifting from traditional data centers to public cloud is one of the main reasons for not complying with the law. The official of the Ministry of Trade stated that PayPal's representative told them that they have no problem with investing in Turkey, but they do not approve localization requirements in itself[179].

According to the 2014 report of The Economic Policy Research Foundation of Turkey (TEPAV[180]), that was published before the exit of PayPal, warned that the localization requirements for payment services might affect the cross border sales, may result in the exit of current players and prevent new players from investing in Turkey[181].

[176] 'PayPal's CTO on Why the Digital Payment Company Relies on Google Cloud' <https://www.youtube.com/watch?v=-Q5uMKPAqw0> accessed 2 May 2020.
[177] 'BDDK'dan "PayPal" Açıklaması' (2016) <https://www.aa.com.tr/tr/ekonomi/kanuna-uygun-olmadigindan-paypalin-lisans-basvurusu-onaylanmadi/582825> accessed 2 May 2020.
[178] PayPal, 'PayPal Turkey Privacy Policy' (2015) <https://www.paypal.com/tr/webapps/mpp/ua/privacy-full?locale.x=tr_TR#6>.
[179] Çiğdem Koşan, Information Security and Cryptography Conference, Middle East Technical University, 3-4 December 2020
[180] TEPAV was established by a group of business people, bureaucrats and academicians for the purposes of conducting data-based policy analysis and policy making contributions. https://www.tepav.org.tr/en/html/249/About+us/"
[181] Ussal Şahbaz, Ali Sökmen and Ayşegül Aytaç, 'Türkiye'de e - İhracat' (2014) 32."

According to a report of eBay, 84% of the Turkish firms used PayPal in exporting products to 175 different countries[182]. More than %50 of all the exports were made to United States (33%), Germany (12%), and United Kingdom (6%)[183]. The report indicates that the top 5% of the exporters of PayPal corresponded to 39% of the total exports, whereas this is 78% for the top 5% of traditional exporters. This shows us that the usage of PayPal was beneficial for SMEs as it was with big corporations[184].

The exit of PayPal from Turkey affected many people who were outspoken at online platforms explaining their hardship in doing business internationally and finding alternative ways to receive funds[185]. Most of the complaints were made by people who could not receive funds from abroad, lost their freelance jobs, and could not sell or purchase products[186]. UTIKAD, a Turkish NGO representing more than 450 companies in the logistics sector, identifies the exit of PayPal as one of the problems that decrease the cross border e-commerce sales[187]. The official of the Ministry of Trade stated that they had received many complaints from exporters and SMEs regarding the localization rules of BRSA that resulted in the exit of PayPal[188].

The exit of PayPal accelerated domestic payment providers' development, such as BKM, Papara, and Iyzico. However, these new players are not sufficient to replace the gap of cross border payments that PayPal filled since they are not widely used abroad. Transferwise entered the Turkish payment market with a business model that relies on a Turkish company[189] to process its local transactions, and it has the

[182] ebay inc, 'Commerce 3.0: A Springboard for Turkey's Small Businesses to the Global Economy' (2014) 2.
[183] ibid 5.
[184] ibid 13.
[185] An official request was made to PayPal for obtaining the following information: amount of remittances received to accounts in Turkey until June 2016, amount of remittances sent by accounts in Turkey until June 2016, and ratio of remittances received from and sent to Turkey. However no response was given.
[186] Ekşi Sözlük, 'Paypal - Entries' <https://eksisozluk.com/paypal--252633?p=170> accessed 31 August 2020.
[187] Uluslararası Taşımacılık ve Lojistik Hiztmet Üretenleri Derneği (UTIKAD), 'Türkiye'de E-Ticaret ve E-Ihracat Gelişim Potansiyeli ve Lojistik Süreçler' (2019) 14.
[188] 'Koşan' (n.178)
[189] Birleşik Ödeme Hizmetleri ve Elektronik Para Anonim Şirketi" is processing the transactions of Transferwise in locally installed databases.

potential to be beneficial for the ones who send and receive funds outside of Turkey. However, no data is suggesting that its entrance to the Turkish market filled the gap of PayPal.

Turkey's policy requiring the payment services to install data centers' inside the country forced PayPal to exit the market. There might be various motivations behind this policy, such as law enforcement, economic security, data security, or promoting local payment providers. Most of these reasons might have been satisfied with various solutions. Mandatory access, as required in international agreements, could have been implemented with high penalties, the data protection rules might have been applied to ensure data security, and the sovereignty might be extended by devising data access agreements to bypass the pre-existing Mutual Legal Assistance Treaties (MLAT) and reach the data directly from where it is stored. Forcing PayPal to exit might help build a domestic payment market, but on the other hand, the function in enabling cross-border payments and the pace of development in the payment market were interrupted. The recent developments in the open banking era shows us that building a strong payment market is only possible by providing a business-friendly, data-sharing ecosystem. The payment market is not a winners take all market, with several banks and stunning technological developments. This was proved in many countries, and the business-friendly environment enabled payment services to thrive even in the presence of companies like PayPal. On the opposite, requiring the payment services to bear more costs by installing data centers within the country would help major players who are more capable of covering such costs. This requirement also prevents domestic players from reaching and competing in foreign markets.

PayPal might have decided to comply with the localization rules and operate in a dynamic market with an +80 million population besides the 200 different countries they are in business. Nevertheless, the global trend of shifting the infrastructure from traditional data centers to the cloud is a reality that the regulators must adopt. The exit of PayPal turned an easy win-win into a lose-lose situation.

CONCLUSION

This research aimed to answer the following questions:

1 – What is the importance of cross-border data flows?

2 - How do Turkey, EU, India, China, and Russia handle data?

3 – Are special rules applied for financial institutions in respect of data practices? If so, what are they, and how are they implemented?

4 – Overall, where is Turkey positioned? What are the rules, practices, and outcomes of such rules?

5 – What is the effect of data localization rules on the economy and financial industry?

In order to answer these interdisciplinary and interlinked questions, this research first emphasized the importance of data to the world economy and examined the international agreements and multilateral/bilateral trade agreements as a sign to show the importance of cross border data transfers.

The second part used the categorization of *Ferracane* in dividing the localization regimes and applied them to the selected countries and blocks in the third section. By examining the legal framework of the selected countries, it was aimed to show the rules and practices of financial institutions. Since the EU framework influenced the Turkish legislations, special attention was brought in comparing both practices. It was determined that the legal framework of banks, payment services, and electronic money institutions in Turkey are not compliant with PDPL, and there are overlapping issues that must be addressed. As a result of the examination, Turkey was determined to have the strictest rules after China. This alone shows that the direction of Turkey is contradictory with the European practice in handling financial data.

In the fourth section, the economic effect of localization rules was analyzed using the available data. It was proved that the localization rules negatively affect nearly every country with different portions. The GDP, welfare, investment, export,

import, production, FDI, new job creation, and energy market and environment were analyzed, and it was concluded that the more the economy is data-driven, the more the nations are affected.

According to the reports, one of the most restricted data is financial data, and the most affected sector is the financial industry. Thus, the impact of such rules on the financial industry was significant. The localization rules increases the costs of financial institutions' IT infrastructure by preventing them from using public cloud providers and spending considerable sums to install or use local data centers. This also forces the institutions to focus on a side business instead of allocating those duties to third party providers. The localization requirements prevents financial institutions from using cloud-based products and new technologies. They also prevent Turkish fintechs/banks from competing in the international market due to the heavy burdens, lack of technology, security products, and unflexible IT structure. While most financial institutions in the developed world switched their infrastructure to cloud, enjoy improved security products, and collaborate internationally, Turkish banks and fintechs have limited capacity in participating in the global sphere.

The increasing costs of payment services and restrictions on cross-border transfers also affect the e-commerce sector by increasing the products' price. The lack of international payment services due to localization requirement decreases the competitive advantage of e-commerce platforms in the international e-commerce market.

The globalization made it easier to send and receive remittances between the countries. But the costs of cross-border money remittance fees are still very high, based on the United Nations' target of 3%. Decreasing cross-border money remittance fees would be possible due to innovative solutions, decreasing the unnecessary costs, benefiting from the technological developments, and collaborating on an international level. Forcing the banks/fintechs to localize the data will interrupt the efforts.

The localization rules may also force the international providers to exit the country. In the final section, a concrete outcome of the localization rules was examined, i.e., PayPal's exit from the Turkish market.

Localization rules do not only harm the Turkish economy; they also restrict the ability of the Turkish banks, fintechs, and financial institutions to compete in the global arena and bring innovation to the market. The disruptive nature of technology requires adaption, which will add to the economy and welfare of the public. The conventional security methods are outdated, and new approaches must be devised to defend intelligent and targeted cyberattacks. Many experts agree that it would be wise to focus on the product itself rather than the outdated security requirement that exceeds the aim of data protection.

Although there is considerable effort to modernize Turkey's financial industry, these efforts might be undermined as the technologies develop at high speed. Furthermore, the strict localization rules might also restrict Turkey's ability to negotiate, devise or enter into trade agreements as more and more countries are including the ban of data localization practices in the agreements.

BIBLIOGRAPHY

Accenture, ‘HOW ARTIFICIAL INTELLIGENCE CAN DRIVE CHINA’S GROWTH’ <https://www.accenture.com/cn-en/insight-artificial-intelligence-china>

——, ‘REWIRE FOR GROWTH: Accelerating India’s Economic Growth with Artificial Intellegince’ (*Accenture*, 2017) <https://www.accenture.com/_acnmedia/PDF-68/Accenture-ReWire-For-Growth-POV-19-12-Final.pdf>

AGARWAL S, ‘WHY ISO 20022 IS A SEISMIC SHIFT FOR PAYMENTS’ (*Accenture*, 2020) <https://bankingblog.accenture.com/iso20022-seismic-shift-payments> accessed 22 November 2020

‘Agreement between the United States of America, the United Mexican States, and Canada 12/13/19 Text’ (2018) <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>

Alison DeNisco Rayome, ‘Why Data Centers Fail to Bring New Jobs to Small Towns - TechRepublic’ (2016) <https://www.techrepublic.com/article/why-data-centers-fail-to-bring-new-jobs-to-small-towns/> accessed 20 July 2019

Australian Government Department of Foreign Affairs, ‘CPTPP Outcomes: Trade in the Digital Age’ <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/outcomes-documents/Pages/cptpp-digital>

——, ‘TPP Outcomes: Financial Services’ <https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/outcomes-financial-services> accessed 5 October 2020

Azmeh S and Foster C, ‘The TPP and the Digital Trade Agenda: Digital Industrial Policy and Silicon Valley’s Influence on New Trade Agreements’ (2016) 44 London School of Economics 35 <http://www.lse.ac.uk/internationalDevelopment/home.aspx>

Bada D and Okumuş Yavuzdoğan B, ‘Turkey’s New Data Storage and Transfer

Requirements for Banks' (*iapp*, 2020) <https://iapp.org/news/a/turkeys-new-data-storage-and-transfer-requirements-for-banks/> accessed 2 October 2020

Basu A, Hickok E and Chawla AS, 'The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India' [2019] The Centre for Internet and Society <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf>

Bauer M and others, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (2014) 32 ECIPE occasional paper <https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf>

——, 'Data Localisation in Russia: A Self-Imposed Sanction' (2015)

Bauer M, Ferracane MF and Marel E Van Der, 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization'

'BDDK'dan "PayPal" Açıklaması' (2016) <https://www.aa.com.tr/tr/ekonomi/kanuna-uygun-olmadigindan-paypalin-lisans-basvurusu-onaylanmadi/582825> accessed 2 May 2020

Beattie A, 'Data Protectionism: The Growing Menace to Global Business' *Financial Times* (2018) <https://www.ft.com/content/6f0f41e4-47de-11e8-8ee8-cae73aab7ccb>

Bilgic S, 'SOMETHING OLD, SOMETHING NEW, AND SOMETHING MOOT: THE PRIVACY CRISIS UNDER THE CLOUD ACT' (2018) 32 Harvard Journal of Law & Technology

Bird J, 'Cloud Is Silver Lining for German Online Bank Fidor' *Financial Times* <https://www.ft.com/content/4eea4798-81c6-11e3-87d5-00144feab7de>

Botta A and others, 'PSD2 : Taking Advantage of Open- Banking Disruption' (2018)

Brodsky L and Oakes L, 'Data Sharing and Open Banking' (2017)

BuzzFeed News, '8 Things You Need To Know About The Dark Side Of The World's Biggest Banks, As Revealed In The FinCEN Files' (2020)

<https://www.buzzfeednews.com/article/jasonleopold/fincen-files-8-big-takeaways> accessed 7 October 2020

Cisco, 'Cisco Annual Internet Report' (2020)

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 'A Free and Fair Digital Economy Protecting Privacy , Empowering Indians'

Cory N, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?' (2017) <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>

Council of Europe, 'Chart of Signatures and Ratifications of Treaty 108' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=w4NkUCsR> accessed 18 September 2020

——, 'Chart of Signatures and Ratifications of Treaty 223' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures> accessed 23 September 2020

Creemers R, Triolo P and Webster G, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' (*New America*, 2018) <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/> accessed 28 August 2020

Danish Energy Agency, 'Denmark's Energy and Climate Outlook 2019' (2019)

Desai RD, 'India's Data Localization Remains A Key Challenge For Foreign Companies' (*Forbes*) <https://www.forbes.com/sites/forbesleadershipteam/2020/08/10/business-as-unusual/#6e38931a24d5>

Dillet R, 'France's Health Data Hub to Move to European Cloud Infrastructure to Avoid EU-US Data Transfers' (2020) <https://techcrunch.com/2020/10/12/frances-health-data-hub-to-move-to-european-cloud-infrastructure-to-avoid-eu-us-data-transfers/> accessed 13

October 2020

ebay inc, ‘Commerce 3.0: A Springboard for Turkey’s Small Businesses to the Global Economy’ (2014)

Ecommerce Foundation, ‘Global Ecommerce Report 2017’ (2017)

Eduardo Ustaran, *European Data Protection Law and Practice* (International Association of Privacy Professionals (IAPP) 2018)

EIRGRID, ‘All-Island Generation Capacity Statement - 2019-2028’ (2019)

European Commission, ‘Adequacy Decisions’ <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>

——, ‘A European Strategy for Data’ (2020) <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf>

Fefer RF, ‘TPP Financial Services Data Flows’ <https://fas.org/sgp/crs/row/IN10498.pdf>

Ferracane M, ‘Restrictions on Cross-Border Data Flows: A Taxonomy’ [2018] SSRN Electronic Journal 1

Findlay S, ‘India Bans Dozens of Chinese Mobile Apps’ *Financial Times* (2020) <https://www.ft.com/content/08e15c26-48e0-4540-a040-1a8782e84f2e>

Guardian, ‘The Cambridge Analytica Files’ *Guardian* (2018) <https://www.theguardian.com/news/series/cambridge-analytica-files>

HADANO T and NAKANO T, ‘Xi Says China Will Consider Joining TPP’ (*Nikkei Asia*, 2020) <https://asia.nikkei.com/Politics/International-relations/Xi-says-China-will-consider-joining-TPP> accessed 21 November 2020

Hardy Q, ‘Cloud Computing Brings Sprawling Centers, but Few Jobs, to Small Towns - The New York Times’ (2016) <https://www.nytimes.com/2016/08/27/technology/cloud-computing-brings-

sprawling-centers-but-few-jobs-to-small-towns.html> accessed 20 July 2019

Helgadottir D, ‘The Conflict Concerning Data Sharing under PSD2 and Obtaining Consent to Share Such Data under GDPR’ (*University of Oxford Faculty of Law*, 2020) <https://www.law.ox.ac.uk/business-law-blog/blog/2020/07/conflict-concerning-data-sharing-under-psd2-and-obtaining-consent> accessed 4 October 2020

Hemmings, Justin and Srinivasan, Sreenidhi and Swire, Peter, Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act (October 7, 2019). Journal of National Security Law and Policy, Forthcoming, Georgia Tech Scheller College of Business Research Paper No. 3469808, Available at SSRN: https://ssrn.com/abstract=3469808

——, ‘THE INTERACTION BETWEEN DIRECTIVE 2015/2366 (EU) ON PAYMENT SERVICES AND REGULATION (EU) 2016/679 ON GENERAL DATA PROTECTION CONCERNING THIRD PARTY PLAYERS’ (2020) 23 Trinity College Law Review 201

HFW, ‘China: Cybersecurity Law and Data Localisation - Lexology’ (2018) <https://www.lexology.com/library/detail.aspx?g=ee05d71c-fe7f-44ca-87ce-6ae0afb74071> accessed 18 May 2020

Intel, ‘Selecting a Data Center Site: Intel’s Approach’ (2014)

Investopedia, ‘Coopetition’ <https://www.investopedia.com/terms/c/coopetition.asp>

——, ‘Introduction to the Solow Residual’ (*Investopedia*) <https://www.investopedia.com/terms/s/solow-residual.asp> accessed 18 May 2020

——, ‘Process Value Analysis (PVA)’ <https://www.investopedia.com/terms/p/process-value-analysis-pva.asp> accessed 18 May 2020

Kalra A, ‘Mastercard Says Storing India Payments Data Locally in Face of New

Rules' (*Reuters*, 2018) <https://cn.reuters.com/article/india-data-localisation-mastercard-idCNL3N1XA5JH>

Kamiya G and Oskar K, 'Data Centres and Energy – from Global Headlines to Local Headaches?' (2019) <https://www.iea.org/commentaries/data-centres-and-energy-from-global-headlines-to-local-headaches>

KPMG, 'The Truth about Online Consumers - 2017 Global Online Consumer Report' (2017) <https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/01/the-truth-about-online-consumers.pdf>

Lee J, Arons S and Comfort N, 'European Banks Store Their Sensitive Data on American Clouds' (*Bloomberg Businessweek*, 2020) <https://www.bloomberg.com/news/articles/2020-03-06/european-banks-store-their-sensitive-data-on-american-clouds?utm_source=url_link>

Linklaters, 'PBOC Publishes New Data Protection Guidelines for Financial Institutions' (2020) <https://e.linklaters.com/67/921/downloads/20200304-pboc-publishes-new-data-protection-guidelines-for-financial-institutions.pdf>

Mamdouh A and others, 'Exploring International Data Flow Governance Platform for Shaping the Future of Trade and Global Economic Interdependence' (2019) <http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf>

Mckinsey Global Institute, 'Digital Globalization: The New Era of Global Flows' (2016) <https://www.mckinsey.com/~/media/McKinsey/Business Functions/McKinsey Digital/Our Insights/Digital globalization The new era of global flows/MGI-Digital-globalization-Full-report.ashx>

Miller R, 'The Economics of Data Center Staffing | Data Center Knowledge' <https://www.datacenterknowledge.com/archives/2008/01/18/the-economics-of-data-center-staffing> accessed 4 May 2020

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY Department of Information Technology, 'Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011' <https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>

Morgan JP, ‘J.P. Morgan Interbank Information Network® Grows to 300+ Banks’ (2019) <https://www.jpmorgan.com/country/US/EN/detail/1320575182345>

Navarro P, ‘French Court Refuses to Suspend Microsoft’s Hosting of a Public Health Data Lake despite CNIL Opinion’ (*Hogan Lovells*, 2020) <https://www.engage.hoganlovells.com/knowledgeservices/news/french-court-refuses-to-suspend-microsofts-hosting-of-a-public-health-data-lake-despite-cnil-opinion-the-health-data-hub-case-part-2> accessed 29 October 2020

Noonan L, ‘Swift Takes on Fintechs with New Payment System’ (2018) <https://www.ft.com/content/05d41660-f7c8-11e8-af46-2022a0b02a6c>

Norton Rose Fulbright, ‘PBOC Issues New Specification on Personal Financial Information’ (*March*, 2020) <https://www.nortonrosefulbright.com/en-gb/knowledge/publications/fcdc5f10/pboc-issues-new-specification-on-personal-financial-information> accessed 28 August 2020

O’Conner B, ‘Quantifying the Cost - Interactive Data Visualization’ <http://cloudsecurity.leviathansecurity.com/> accessed 9 May 2020

O’Connor B, ‘Leviathan Security Group - Quantifying the Cost of Forced Localization’ (2015) <https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf>

‘PayPal’s CTO on Why the Digital Payment Company Relies on Google Cloud’ <https://www.youtube.com/watch?v=-Q5uMKPAqw0> accessed 2 May 2020

PayPal, ‘PayPal Turkey Privacy Policy’ (2015) <https://www.paypal.com/tr/webapps/mpp/ua/privacy-full?locale.x=tr_TR#6>

——, ‘PayPal 2019 Annual Report’ (2020) <https://investor.paypal-corp.com/static-files/6b4a31d7-9941-464d-846d-3859fd7058dc>

‘PayPal Partners with Google Cloud’ (2018) <https://www.youtube.com/watch?time_continue=30&v=9jJ6xLOSS3c&feature=

emb_logo> accessed 2 May 2020

Penn D, ‘PayPal Takes to the Google Cloud - Finovate’ <https://finovate.com/paypal-takes-to-the-google-cloud/> accessed 1 May 2020

Piper D, ‘DATA PROTECTION LAWS OF THE WORLD’ <https://www.dlapiperdataprotection.com/index.html?t=law&c=RU&c2=TR>

Presidencey of the Republic of Turkey, ‘11th Development Plan’ (2019)

Rauwald C, Ozsoy T and Ersoy E, ‘Volkswagen Turkey Unit Paves Way for $1.4 Billion Plant - Bloomberg’ <https://www.bloomberg.com/news/articles/2019-10-02/volkswagen-establishes-unit-to-manufacture-cars-in-turkey> accessed 3 May 2020

Reinsel D, Gantz J and Rydning J, ‘The Digitization of the World - From Edge to Core’ (2018) <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>

Reserve Bank of India, ‘Reserve Bank of India - Frequently Asked Questions’ <https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130> accessed 28 August 2020

——, ‘Storage of Payment System Data’ 1 <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF>

Reuters, ‘Turkey’s Akbank Faces $4 Million Hit from Attempted Cyber Heist’ (2016) <https://www.reuters.com/article/us-akbank-cyber-idUSKBN1450MC>

Rosenwald MS, ‘Cloud Centers Bring High-Tech Flash but Not Many Jobs to Beaten-down Towns - The Washington Post’ (2011) <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> accessed 3 May 2020

Şahbaz U, Sökmen A and Aytaç A, ‘Türkiye’de e - İhracat’ (2014)

Scharwatt C, ‘The Impact of Data Localisation Requirements on the Growth of Mobile Money-Enabled Remittances’ (2019)

Schwartz P and Karl-Nikolaus P, ‘Data Localization Under the CLOUD Act and the GDPR’ (2019) 1 Computer Law Review International

Scottish Government, ‘Computable General Equilibrium Modelling: Introduction’ (2016) <https://www.gov.scot/publications/cge-modelling-introduction/>

Singh M, ‘Trump Bans US Transactions with Chinese-Owned TikTok and WeChat’ *Guardian* (2020) <https://www.theguardian.com/technology/2020/aug/06/us-senate-tiktok-ban>

Solow RM, ‘Nobel Prize Lecture: Growth Theory and After’ <https://www.nobelprize.org/prizes/economic-sciences/1987/solow/lecture/> accessed 18 May 2020

Sözlük E, ‘Paypal - Entries’ <https://eksisozluk.com/paypal--252633?p=170> accessed 31 August 2020

Tai K and others, ‘Translation: China’s New Draft “Data Security Management Measures”’ (*New America*, 2019) <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/> accessed 28 August 2020

The Grand National Assembly of Turkey, ‘Law on The Protection of Personal Data No. 6698’ <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>

‘Trans-Pacific Partnership Agreement’ (2016) <https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/tpp-text-and-associated-documents>

TÜBİSAD, ‘Türkiye’de E-Ticaret 2018 Pazar Büyüklüğü’ (2019) <http://www.tubisad.org.tr/tr/images/pdf/tubisad_2019_e-ticaret_sunum_tr.pdf>

Turkish Data Protection Authority, ‘Announcement of DPA on Binding Corporate Rules’ <https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU> accessed 9 May 2020

——, ‘Decision of DPA Dated 27 February 2020 and No. 2020/173 Regarding

Amazon Turkey' <https://kvkk.gov.tr/Icerik/6739/2020-173> accessed 9 May 2020

——, 'Summary of the Decision of the Personal Data Protection Board Dated 22/07/2020 and Numbered 2020/559 Regarding "the Transfer of Personal Data Abroad on the Basis of Convention No. 108"' <https://kvkk.gov.tr/Icerik/6812/2020-559>

——, 'Announcement on Cross-Border Transfer' (2020) <https://kvkk.gov.tr/Icerik/6828/YURTDISINA-VERI-AKTARIMI-KAMUOYU-DUYURUSU> accessed 29 October 2020

U.S. Chamber of Commerce Internation Affairs, 'Globally Connected, Locally Delivered: The Economic Impact of Cross-Border ICT Services' (2016)

U.S. International Trade Comission, 'Digital Trade in the U.S. and Global Economies - Part 2' 331 <http://www.usitc.gov/publications/332/pub4485.pdf>

UK Government, 'UK and Japan Agree Historic Free Trade Agreement' (*2020*) <https://www.gov.uk/government/news/uk-and-japan-agree-historic-free-trade-agreement> accessed 24 September 2020

Uluslararası Taşımacılık ve Lojistik Hiztmet Üretenleri Derneği (UTIKAD), 'Türkiye'de E-Ticaret ve E-Ihracat Gelişim Potansiyeli ve Lojistik Süreçler' (2019)

UNCTAD, 'UNCTAD Estimates of Global E-Commerce 2018' (2020) <https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d12_en.pdf>

Vidal J, '"Tsunami of Data" Could Consume One Fifth of Global Electricity by 2025' *Climate Home News* (2017) <https://www.climatechangenews.com/2017/12/11/tsunami-data-consume-one-fifth-global-electricity-2025/>

Voigt P and Von dem Bussche A, *The EU General Data Protection Regulation (GDPR)* (Springer 2017)

Wei Y, 'Chinese Data Localization Law: Comprehensive but Ambiguous - The

Henry M. Jackson School of International Studies' (2018) <https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/> accessed 28 August 2020

World Bank, 'Data Release: Remittances to Low- and Middle-Income Countries on Track to Reach $551 Billion in 2019 and $597 Billion by 2021' (2019) <https://blogs.worldbank.org/peoplemove/data-release-remittances-low-and-middle-income-countries-track-reach-551-billion-2019>

World Economic Forum, 'A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy' (2020)

Yapıkredi, 'E-Posta Gönderimlerindeki Değişiklikler Hakkında Bilgilendirme' (2020) <https://www.yapikredi.com.tr/e-posta-bilgilendirme> accessed 28 August 2020

Zhang G and Yin K, 'A Look at China's Draft of Personal Data Protection Law' (*iapp*, 2020) <https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/> accessed 30 October 2020

PRESS RELEASE No 91 / 20 The Court of Justice invalidates Decision 2016 / 1250 on the adequacy of the protection provided by the EU-US Data Protection Shield (2020) C-311/18

Banking Regulation and Supervision Agency, Regulation on the Management and Auditing of the Information Systems Used By the Payment and Electronic Money Institutions 2014 1

——, Draft Communiqué on Remote Identification Methods to be used by Banks 2020

——, Regulation on Banks' Information Technology and Electronic Banking Services 2020

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

——, Explanatory Report to the Convention for the Protection of Individuals with

regard to Automatic Processing of Personal Data 1981

——, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (Treaty No.108) 2001

European Banking Authority, Recommendations on outsourcing to cloud service providers 2017 1

European Union, REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union 2018 1

Justice and Development Party (AK Parti), The Reasoning of Amendment Law 2020

The Central Bank of the Republic of Turkey, Regulation on the Generation and Use of the Turkish QR Code in Payment Services 2020

The Grand National Assembly of Turkey, Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions No. 6493

Turkey TGNA of, Amendment on Banking Law and other laws 2020

Turkish Data Protection Authority, Announcement of DPA on the important points that must be evaluated when preparing the undertakings for transferring data abroad

Convention for the protection of individuals with regard to the processing of personal data (Convention 108+) 2018

CONVENTION ON MUTUAL ADMINISTRATIVE ASSISTANCE IN TAX MATTERS 1988

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC