Global Journal of human-social science: H Interdisciplinary
Volume 21 Issue 9 Version 1.0 Year 2021
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-460x & Print ISSN: 0975-587X

Data Protection Laws Trends: *Practice and Debate*

By Hedaia-T-Allah Nabil Abd Al Ghaffar

Cairo University

Abstract- Technological advancement changed the way everything is being done, providing extraordinary benefits and low costs. People and governments are increasingly adopting new technologies to achieve better performance and financial savings. However, those benefits do not come at no cost; technological advancements (such as Cloud Computing, Artificial Intelligence, Robotics, Internet of Things,..etc) involve several security challenges that may expose countries' national securities. The touchstone in this is data. Data has always been central to national security throughout different historical periods. Intelligence agencies' core of work has always been data; however, the mechanisms of getting and securing data evolved throughout history. Nowadays, the applications of different technologies generate enormous amounts of data that are stored in data centers located in different countries. Data could be traveling across countries and between data centers in a routine process so as to balance loads between data centers of the company. This process contains several security risks because countries lose control and sovereignty over the data generated or collected inside their territories, which exposes the core of nation's sovereignty and national security.

Keywords: data protection, data localization, general data protection regulation, national security, sovereignty, conditional flow of data, privacy shield.

GJHSS-H Classification: FOR Code: 270707

Strictly as per the compliance and regulations of:

Data Protection Laws Trends: *Practice and Debate*

Hedaia-T-Allah Nabil Abd Al Ghaffar

Abstract- Technological advancement changed the way everything is being done, providing extraordinary benefits and low costs. People and governments are increasingly adopting new technologies to achieve better performance and financial savings. However, those benefits do not come at no cost; technological advancements (such as Cloud Computing, Artificial Intelligence, Robotics, Internet of Things,..etc) involve several security challenges that may expose countries' national securities. The touchstone in this is data. Data has always been central to national security throughout different historical periods. Intelligence agencies' core of work has always been data; however, the mechanisms of getting and securing data evolved throughout history. Nowadays, the applications of different technologies generate enormous amounts of data that are stored in data centers located in different countries. Data could be traveling across countries and between data centers in a routine process so as to balance loads between data centers of the company. This process contains several security risks because countries lose control and sovereignty over the data generated or collected inside their territories, which exposes the core of nation's sovereignty and national security. This has led states to draft data protection regulations to make sure they keep the data of their citizens and governmental agencies under best control and immune from infringements. In doing this, countries developed different approaches and patterns for data protection. This paper aims at mapping worldwide trends in data protection regulations, highlighting main worldwide models that other countries follow or create their mixtures. Debates about those trends and their implications are highlighted afterwards, and finally some broad criteria are provided so as to benchmark different data protection laws. The paper is theoretically based on the general underpinning of neocolonialism; in the sense that controlling data of nations may be a new form of practicing colonialism and control over countries instead of the traditional political and economic instruments, especially due to the great benefits gained from new technologies that tempt citizens and governments to adopt.

Keywords: data protection, data localization, general data protection regulation, national security, sovereignty, conditional flow of data, privacy shield.

I. Introduction

Data has always been an important resource and the main focus of countries' national security. In an extremely connected world, data generated by new technologies became even more important and in great need to be protected. On the other hand, today's technologies, which contribute greatly to the worldwide economy, are based on the generation of data that is the basis for the Internet and for the growth of Artificial Intelligence, Big Data, Internet of Things, Cloud Computing and other technologies. Balancing between protecting national security while benefiting from new technologies is an extremely difficult task, especially in light of the security risks presented by new technologies that require transferring data across borders. One of the methods countries resorted to in order to achieve both targets is drafting data protection laws and regulations to protect national data from breaches and disclosure. However, countries took several ways and developed different models of data protection laws, some of which infused international debate. Building upon previously published research about government cloud computing and national security [1], the paper tries to answer a simple research question revolving around how do countries differ in protecting their data and national security. The paper tackles the topic of data protection trends between practice and debate; mapping international models and trends of data protection, shedding light on current debates in this regard, and finally presenting some broad guidelines that can help countries choose the most suited data protection alternative.

II. Mapping Data Protection Worldwide Trends

a) *The European Model (GDPR)*

The European Union has been regulating data protection in a very strict way over the years. The General Data Protection Regulation (GDPR) is the current law regulating data protection in EU. It came into effect on the 25th of May 2018 after being approved by the EU Parliament on the 8th of April 2016. By approving GDPR, the predecessor Data Protective Directive, which was regulating data protection in EU since 1995, was consequently obsolete [2]. Even though the Data Protective Directive was doing well-protecting data in the EU, the European data was prone in the last years to several violations, which led to developing the GDPR.

The new GDPR aims at empowering European citizens to control their personal data in a more effective way, in addition to unifying laws regulating data transfer and protection among all European countries, given the fact that the predecessor Data Protection Directive was

Author: Ph.D in Political Science (Comparative Political Systems) – Faculty of Economics and Political Science- Cairo University- Cairo-Egypt. e-mail: hedaia2008@live.com

not compulsory to EU countries, but more of a non-binding framework. This situation witnessed change with the GDPR, which is binding and compulsory to all EU countries. The GDPR is not only compulsory to European countries but to all other companies and institutions in whatever place, so long as they deal with European citizens' data. The following summarizes main rights guaranteed to European citizens through the GDPR: [3], [4]

- *Increased territorial scope:* Increasing the law's territorial scope is considered one of the major changes that affected the EU data regulatory framework. This goes back to the fact that the new GDPR applies to all companies working with storing and processing personal data of individuals residing in the EU, irrespective of the place of the company. In fact, this came as a remedy to the situation created by the predecessor Data Protection Directive, which was silent and vague about the territorial applicability of the directive. This led to filing many suits about whether to apply the directive or not in different cases. Therefore, the GDPR came out much stronger, compulsory and very clear regarding the territorial applicability of the law. Additionally, non- European data controllers and processors* who process or store European citizens' data are obliged to nominate a representative of the EU, as per Article 3-3 (Official Journal of the European Union: 32,33).
- *Penalties:* One of the most important modifications that were introduced by the GDPR is imposing penalties for the violators; the penalty could reach a maximum of 4% of annual revenue or 20 million euro (whatever is greater), which is the maximum penalty imposed for the strong violations. The penalties system created by the GDPR follows a tiered approach to fines, according to the type of violation. (Article 83)
- *Consent:* The consent of users is firmly regulated in the GDPR, so that the wording of the terms of the agreement should be readable and easily written. Also, the reason for processing data should be clearly stated as well. Most importantly, according to the GDPR, users should have the right to withdraw their consents whenever they want. (Article 7)
- *Breach notification:* The GDPR considers breach notification, within a maximum of 72 hours of finding out 'without undue delay', as a compulsory activity that should be carried out in response to witnessing data breaches, as it endangers users' data integrity and security. (Articles 33,34)
- *Right to access:* The GDPR guarantees the right of the users to get a confirmation from the data controller if their data is being processed or not, and for what reasons. This is in addition to guaranteeing users' rights to get an electronic version of their personal data at the data controller, without any expenses, which is considered a new form of empowering users and securing data.
- *Right to be forgotten/Data erasure:* The GDPR guarantees the right of users to force the data controller to erase their personal data and to stop collecting more data about them whenever the purpose of collecting data comes to an end, whenever the users withdraw the consent they gave in before collecting their personal data and processing it.

On a side note, it is worth mentioning that the GDPR regulates personal data in the EU. Meanwhile, there is the Regulation on the Free Flow of Non-Personal Data that regulates non-personal data in the European Union. Both of the regulations are being applied side by side to create a unified digital single market.

b) The United States Model

The Snowden revelations showed an unstable relationship between IT giant companies and the American security apparatus, based on imposed obligations on IT giant tech companies to reveal users' data so long as data centers are located on the American lands or processed by American companies located outside American territories. This activity is done by means of judicial approval by relevant courts.

These acts led many countries to consider the American companies as untrusted and that their citizens' data are unsafe in their hands. Several counter-reactions have been taken by countries, as will be clear later in the paper. Additionally, disputes were raised between giant tech companies and the American security apparatus, as companies were trying to find ways out of the diminishing trust they are suffering from, creating pressure on American authorities to amend the laws in this regard. Some tech companies, such as Microsoft, sued American authorities for obligations to reveal users' data in Ireland. Also, following the Snowden revelations scandal, IBM started investing billions of dollars for building more than 15 data centers around the world. [5]

No doubt that the American data protection laws are considered loose in comparison to the EU GDPR. In fact; as it is the case with many areas, there is no one common law that all states should be following, but several laws and acts on the federal level, in addition

*It is worth mentioning that the cloud computing environment allows third parties to work with the data, so the data controller may be the same as the data processor and may be a third party. For more information about the cloud computing environment, please revise previous research published by the author.

to regulations of states pertaining to data protection of citizens inside those states. Some states are considered stricter than others with firm regulations in data protection, such as Massachusetts, which has strong legislation requiring each institution collecting data to provide a detailed plan of securing data. New York has also passed cybersecurity legislation that imposes a minimum requirement of security level. California is also one of the states known for protecting privacy throughout its history. The California Consumer Act has been recently passed and was put in action in 2020. The Act imposes new obligations on companies related to data protection, such as personal data tiering, clarifying how the data will be used, as well as putting restrictions on sharing personal data. The Act involves data subjects' rights such as the right to access data, the right to be forgotten and the right to refuse to share data with a third party. [6]

To sum up, in the United States of America, there is no one independent entity responsible for protecting data, and there is no one framework for data protection to resort to as well. This has resulted in a loose data protection environment in the USA, which completely contradicts with the strict data protection environment in the European Union. To close this gap between the USA and the EU, the European Union has regulated protecting European data when transferred, processed or stored in the USA in a separate way, through the Safe Harbor Agreement that was in effect in 2000. However, the EU Court of Justice declared the Safe Harbor Agreement obsolete in October 2015, in the wake of the Snowden revelations and the Max Schrems case (the Austrian activist who sued Facebook for disclosing European data to the US security apparatus). These incidents proved the Safe Harbor was not capable of protecting the European data and was therefore replaced by a new law, which is the EU-US Privacy Shield Law in July 2016, to guarantee the maximum data protection for European data.

The main difference between both laws lies in the mechanisms of European data transfer to the USA and the related rights and obligations. Main differences can be outlined as follows: [7],[8],[9]

- Increasing the European citizens' rights; the Privacy Shield provides several ways for EU citizens to file complaints and cases about violations of data protection. The Privacy Shield Panel could be a second resort to file complaints and cases if nothing was reached using the traditional ways.
- Intensifying the rigidity of requirements from American companies to be approved to work with EU data; where companies should get approvals, on individual company basis, to work with EU data according to a list of specifications evaluated by a specific panel. According to the Privacy Shield, American companies should prove their abidance to the specifications on an annual basis, or else they are obliged to destroy all the data held.
- Limiting/Constraining the US government reach to European data; where the American ministry of justice as well as the CIA, are restricted by obligations for not reaching EU data. This should be reviewed on an annual basis.
- The third-party who gets the data transferred to or works with processing European data is totally responsible for data and should undergo the same whole process of accreditation, just as the original party.

c) Data Localization Model

It is becoming a matter of fact that the great development in new technologies is imposing threats on national security, and especially with the data revelations cases and incidents. Countries resorted to several ways to protect their data. One of the widest spread techniques is the data and infrastructure localization. Data localization implies passing laws and regulations that confine storing and processing data inside a specific land or geography, or allowing some specific companies to store and process data. [1]

Even though the European model is considered one form of data localization, the author prefers to consider the data localization as a separate trend; because it contains several versions and iterations. And despite the fact that the EU GDPR is part of the data localization model, the author believes that the GDPR can be considered as a separate trend given the fact that it is the most looked-upon model and many countries around the world drafted their data protection laws after the GDPR model.

Data localization comes in different degrees and forms. Data localization trends can be classified according to the following criteria: [10]

i. *Scope of Application*

Some countries impose a clear data localization policy, including all data of the nation, with a 'general scope of application' such as the EU, Russia [11],[12],[13],[14] and some Latin American countries, that impose data localization obligations on all citizens data (i.e. all data should be stored and processed inside the borders of the country). Other countries applied data localization on data of specific sectors that would harm national security, such as the United States that requires storing sensitive data inside its territories, as well as Canada [15]. This last case is closely attributed to the data tiering mechanism that some countries, such as the United Kingdom and the UAE, resort to in order to mitigate the level of data localization; so that data that are classified as highly sensitive would be localized, while data categorized as less sensitive would move

abroad freely according to concerned laws. The United Kingdom and the UAE impose data localization obligations on health data, for example, as they classify it as highly sensitive data.

Other data and infrastructure localization regulations impose obligations on the importing of IT equipment and require them to be locally produced.

ii. *Level of restrictiveness*

Countries are classified according to the restrictiveness they impose on the transfer of data to several categories, from the strictest to less strict. Studies differ in the number of categories; some classify them into three categories [16], while others classify countries on a continuum of 5 categories [17]. Despite the difference in the number of categories, the core is very similar. The paper adopts the 5-categories classification, as follows:

a. *Strict Localization:* It refers to imposing legal requirements to store and process data in the country, and may potentially include a complete prohibition on cross-border data transfers. It can be said that no one country has applied complete prohibition, but examples of strict regulations are numerous. China has imposed strict data localization requirements for personal information and important data collected by operators of critical infrastructure. Strict (semi-complete) localization requirements in China apply to the health and financial sector. The cybersecurity law in Viet Nam contains a broad and strict localization provision that requires all foreign and domestic suppliers of telecommunications, as well as Internet services (including over-the-top services) offered online to store data locally.

b. *Partial Localization:* Partial localization refers to imposing legal requirements to store data locally, but does not include a prohibition on transferring or storing copies of the data abroad, although specific compliance requirements may be imposed for cross-border data transfer and storage. For example, the Russian Federation and Kazakhstan require companies to store a copy of personal data locally, even if they can otherwise be transferred abroad. So the first two levels are very close, the main difference is whether there is a possibility to transfer copies abroad or not.

c. *Conditional Transfer (Hard/Medium/Soft):* A conditional transfer requirement implies that data can be transferred abroad on conditions of complying with some pre-determined measures. Depending on the design of these compliance requirements, conditional transfers may be categorized as hard, intermediate or soft. Hard compliance measures include strict approvals for transfer, strict regulatory audits, binding corporate rules,..etc. The clearest example is the EU GDPR. Intermediate to soft conditions imply easier compliance requirements, such as the case of Mexico; for transferring personal data abroad, the data protection law of Mexico only requires consent from the users and entering into necessary contracts between data processors and the foreign parties handling the personal data, but no other requirements for prior regulatory approval.

d. *Free Flow of Data:* This pattern implies minimum compliance requirements, or even no one reference for compliance and leaving the floor for companies to ensure data protection. For example, in Canada, any company that transfers personal data abroad is responsible for ensuring compliance with domestic laws, but there are no express restrictions on such transfers. Companies are responsible for designing their template of requirements so as to hold other parties accountable.

Table 1: Regulatory spectrum for cross-border data flows and example countries

Strict data localization	Partial data localization	Conditional transfer: Hard	Conditional transfer: Intermediate/ soft	Free flow of data
Restrictive /Guarded approach		Prescriptive approach		Light-touch approach
China India Indonesia Kazakhstan Nigeria Pakistan Russian Federation Rwanda		Algeria Argentina Armenia Brazil Colombia Cote D'Ivoire Egypt **European Union**	Azerbaijan Bahrain Belarus Ghana Japan Kyrgystan New Zealand Republic of Korea	Australia Canada Mexico Philippines Singapore **United States**

Saudi Arabia	Georgia	United Arab Emirates
Turkey	Israel	
Vietnam	Kenya	
	Malaysia	
	Morocco	
	Peru	
	South Africa	
	Switzerland	
	Thailand	
	Tunisia	
	Ukraine	
	United Kingdom	

Source: UNCTAD (2021)

A light-touch approach implies that all data, including personal data, can generally flow freely across borders with minimal regulatory requirements (if any). The USA is the prominent advocate of this approach.
A prescriptive regulatory approach entails that cross-border data flows are subject to rigorous compliance requirements. The prescriptive approach falls in the middle of the regulatory spectrum, and typically comprises conditional transfer requirements. The EU is the prominent advocate of this approach.
A restrictive regulatory approach means a complete or partial ban on cross-border data flows for reasons of national security and establishing political control over the domestic Internet. A guarded approach focuses on regulatory measures directed towards economic gains and considerations. Both the restrictive and guarded approaches tend to focus primarily on localization regulations, although their predominant policy rationales are quite different.

III. Debate about the Trends

In a data-driven world, where technological products and applications produce huge amounts of data, and with the increasing incidents of data revelations, especially from the side of giant tech companies dominated by the USA, countries are held in a tight position trying not to lose neither the economic benefits and power of new technologies and data-driven economy, nor their sovereignty and control over their people and resources. Countries are being overwhelmed by manifestations of neocolonialism in the technological world. From here, countries resorted to data protection laws and data localization obligations in a way to keep their control over their data and resources. Reasons behind data localization stipulations are fear of dependence, fear of losing control and sovereignty as well as technical concerns emanating from the security breaches, especially when breaches occur outside the territory [1]. One of the strong reasons is the absence of a strong international framework, augmented by frequent breaches scandals from U.S. giant tech companies.

However, data localization laws and regulations led to a wide debate, skewed towards the idea that data localization is an undesirable trend, leading to negative impacts on the global economy and the development of the Internet. On the one hand, the advocates of the trend believe that through confining storing and processing data within the country borders, nations will be able to protect their data from spying and disclosure and would thereby protect their national security. [5]

On the other hand, proponents of this trend believe that these laws usually fail to meet the announced goal and gradually turn to governments spying on their citizens, which impacts democracy and transparency. Most importantly, proponents argue that these kinds of laws negatively impact the growth of the global economy, impede the growth of other technologies that are based on the free flow of data (such as IoT [18], AI and Big Data), as well as threatening the development of Internet and relevant applications. Proponents are afraid that the prevalence of such laws may lead to fragmenting the global Internet infrastructure, which would be a major retreat in the development of the Internet society.[19]

In this regard, Internet Society has recently developed some critical principles upon which the foundations of Internet freedom were based. Internet Society provides training in different countries to support the idea that data localization laws hit the critical principles of the freedom on Internet; precisely Critical Property 1 – An open and accessible infrastructure with a common protocol, Critical Property 3 – Decentralized management and a common distributed routing system and Critical Property 5 – A Technology Neutral, General-Purpose network. [20]

IV. Where to Stand

Given this hot debate, and the wide diversity of data protection trends worldwide, studies developed some guidelines that can work as assessment criteria for countries to assess where to stand in this wide diversity in practice and controversial debates. The paper presents two frameworks for assessing data protection regulations, fulfilling both contradicting views about data localization; protecting national security and allowing for freedom of the Internet, and allowing for assessing the country's specific particularity and

interests as well. Countries are supposed to make the most suitable mix and match from all variables, according to each one's interests, views and strategies.

The first is a group of elements to be assessed regarding data protection stipulations to ensure de jure privacy control and national security. Countries are expected to draft strong data protection regulations so that the following benchmarks apply: [21]

- Severity of requirements in the law that ensure

i) *Control:* individuals have control over their data.
ii) *Safety:* Personal data is safe in the hands of the organizations.

- Severity of compliance mechanisms that ensure

i) *Enforcement:* mechanisms that increase the likelihood of detection
ii) *Sanctions:* strong penalties that deter violations

On the other hand, countries can assess to what extent will data localization benefit the economy through an assessment framework for different localization options. The assessment tool uses scored methodology and takes into consideration several factors for each localization alternative to finally reach a total score for each alternative so as to help the decision-making process [22]. Put simply and concisely, the model measures the impact of data localization alternatives on economic growth and data access, through the following sub-factors:

- Economic growth

i) *Demand for goods and services:* Assessing if building the infrastructure for local storage would create additional demand for goods and services (such as building data centers and the related components) which would consequently lead to creating direct and indirect job opportunities and therefore boost economic growth. However; demand could be affected by the value of imported equipment required for data centers. The overall impact on economic growth would depend on whether the demand would be met through domestic goods or through importing. Weighing those variables would give insights to decision makers about the best option of data protection regulations.

ii) *Competitive advantage of national firms vs. multinational firms:* Countries should assess the costs of data localization from several perspectives. Mandating data localization would require more capital expenditure as a result of the costs of data storage and processing capabilities. Operational expenditure would also increase as a result of the costs of renting or operating data-related infrastructure. Additionally, having to protect data would require additional policy measures. The total cost related to data localization may render multinationals much more competitive than national firms as a result of economies of scale.

iii) *Risk of retaliation against the country's national firms abroad:* The analysis should also measure the risk of other countries retaliating against localization measures taken by the country. Such actions might lead other countries to impose localization restrictions of their own on the other countries' firms that export services.

iv) *Risk of foreign businesses exiting:* Assessing the risk of data loss due to firms choosing to leave or not enter the country due to localization requirements.

- Data access

i) *Scope of access:* Assessing which localization option would grant the country access to the largest amount of personal data. Risk of retaliation is significant in assessing the scope of access. Countries may resort to bilateral or multilateral agreements instead of enforcing localization if this would give more access to data.

ii) *Speed of access:* Since speedy access to personal data is very crucial in crime investigations, speed of access is important in this analysis, since delays can drastically reduce the likelihood of success.

IV. Conclusion

Data protection regulations and data localization trends are some of the most debatable issues in the international arena. The twinning between data protection in the current technological environment and national security is on top of most countries' agendas. The paper presented a mapping of the worldwide trends in data protection, presented the two points of view in this regard, and tried at the end to provide some kind of guidelines for countries to assess the best-suited alternative of data protection. As shown, choosing the optimum level of data security is a tough task, requiring achieving an accurate balance between economic and political considerations to achieve security without harming the economy.

Acknowledgements

This paper and the research behind it would not have been possible without the valuable contributions and support of my dad and supervisor, *Dr. Nabil Abd Al Ghaffar,* PhD in Political Science (Faculty of Economics and Political Science - Cairo University). In the loving memory of my beloved dad who contributed greatly in preparing the original text from which this paper is extracted.

To my beloved mum...Grateful for your love and support.

References Références Referencias

1. Abd Al Ghaffar, Hedaia-T-Allah Nabil (2020). Government Cloud Computing and National Security. Review of Economics and Political Science, ahead of print, DOI: 10.1108/REPS-09-2019-0125
2. Lord, Nate (2018), "What is the Data Protection Directive? The Predecessor to the GDPR", Digital Guardian, available at: https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr
3. EU GDPR.ORG, "Key Changes with the General Data Protection Regulation", available at: https://eugdpr.org/the-regulation/
4. Official Journal of the European Union, Regulation (Eu) 2016/679 Of The European Parliament and of The Council 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), 27 April 2016, p.p. 1-88, available at: https://gdpr-info.eu/
5. Hill, Jonah Force (2014), The Growth of Data Localization Post-Snowden: Analysis and Recommendations For U.S. Policymakers and Industry Leaders, *Lawfare Research Paper Series,* 2(3), 1-41 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430275
6. Chabinsky, Steven, F. Paul Pittman (2019), USA: Data Protection 2019, available at: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
7. Terpan, Fabien (2018), EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?, European Papers, Vol. 3,3 (2018): 1045-1059, available at: http://www.europeanpapers.eu/en/e-journal/eu-us-data-transfer-safe-harbour-privacy-shield
8. OTAVA (2019), COMPARISON Safe Harbor Vs. The EU-US Privacy Shield, available at: https://www.otava.com/reference/how-does-safe-harbor-compare-to-the-eu-us-privacy-shield/
9. Privacy Shield website (2019), available at: https://www.privacyshield.gov/Program-Overview
10. UNCTAD (2021). Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow, https://unctad.org/system/files/official-document/der2021_en.pdf
11. FTI Consulting (2017), Localization to Fragment Data Flows in Asia', available at: https://www.fticonsulting-asia.com/insights/articles/localization-to-fragment-data-flows-in-asia
12. Hogan Lovells (2018), Asia-Pacific Data Protection and Cyber Security Guide available at: https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2018/ab-data-protection-and-cybersecurity.pdf
13. Sauvelyev, Alexander, 'Russian's New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction?, *Computer, Law and Security Review*, 32(2016): 128-145, available at: https://www.sciencedirect.com/science/article/pii/S0267364915001685
14. Savvas, Antony (2019), Internet Iron Curtain Comes Down Across Mother Russia, available at: https://data-economy.com/internet-iron-curtain-comes-down-across-mother-russia/
15. Anupam Chander, Uyen P. Le (2014), "Breaking the Web: Data Localization vs. the Global Internet", *UC Davis Legal Studies Research Paper Series*, (378), available at: http://ssrn.com/abstract=2407858
16. Wu, Emily (2021). Sovereignty and data localization. Belfer Centre for Science and International Affairs. Harvard Kennedy School, available at: https://www.belfercenter.org/publication/sovereignty-and-data-localization#:~:text=Data%20localization%20is%20used%20to%20assert%20data%20sovereignty&text=Generally%2C%20governments%20want%20to%20claim,by%20whom%20it%20is%20stored.&text=It%20is%20generally%20a%20policy,in%20that%20country%20must%20abide.
17. Ferracane, Martina F (2018), "South Africa and Data Flows: How to Fully Exploit the Potential of the Digital Economy", Global Economic Governance Africa, Discussion Paper, https://www.gegafrica.org/publications/92-south-africa-and-data-flows-how-to-fully-exploit-the-potential-of-the-digital-economy
18. GSMA (2021), Cross-border data flows: The impact of data localization on IoT, cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf (gsma.com)
19. Big Bang, Understanding Data Localization Laws, available at: https://www.bigbangerp.com/blog/data-localization-laws/
20. Internet Society (2020), Internet way of networking use case: Data localization, https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-Use-Case-Data-Localization-EN.pdf
21. Nieuwesteeg, Bernold (2016), Quantifying Key Characteristics of 71 Data Protection Laws, Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 7 (2016): 182-203, available at: https://www.jipitec.eu/issues/jipitec-7-3-2016/4510/nieuwesteeg_quantifying%20key_characteristics_of_71_data_protection_laws_jiptec_7_3_2016_182.pdf
22. Burman, Anirudh, Upasana Sharma (2021), How would data localization benefit India?, Carnegie India, https://carnegieindia.org/2021/04/14/how-wo

uld-data-localization-benefit-india-pub-84291#:~:
text=Countries%20limit%20such%20data%20flows
%20in%20multiple%20ways.&text=Advocates%20fo
r%20localization%20in%20India,surplus%20in%20th
e%20Indian%20economy.