Forum:	Special Political & Decolonisation Committee (GA4)
Issue:	The Question of Tech Sovereignty and Data Localisation
Student Officer:	Stergios Stivaktakis
Position:	Co-Chair

PERSONAL INTRODUCTION

Dear All,

My name is Stergios Stivaktakis, and I am currently in Year 11 of the German School of Athens (DSA). I have been involved in Model UN since 2020 through our MUN Club. The world of Model United Nations - as well as the UN itself - interests me greatly, due to addressing societal and political questions.

I have the honour to serve as one of the co-chairs in this year's Special Political and Decolonisation Committee. On that note, it is my pleasure to welcome you to the committee, where we will be discussing issues of paramount importance to our modern society. Through the GA4, our nations find solutions on topics that affect us politically, such as access to data; this study guide's topic.

Being a co-chair of this committee, I wish to work with all its members and help create a series of meaningful discussions on how data localisation affects us, our governments and our national sovereignty, regarding technology. This study guide has been written for you to further your research with a base understanding of the topic. I urge you to use the links and content provided to be prepared for the conference this March.

For any questions that may arise in the meantime, do not hesitate to contact me via email at stergiosstivaktakis@gmail.com.

Sincerely,
Stergios Stivaktakis

INTRODUCTION

Data localisation and tech sovereignty are two interconnected terms of great importance for nations. Data localisation regulations require companies to store and process data locally rather than on servers in other countries. At the same time, tech sovereignty describes a country's ability to align technological activity to its citizens' common interests and needs, including the local storage of essential data.

On one end, as countries move towards digitisation, they often implement localization laws to ensure the proper handling and safeguarding of data. This solution would technically allow a nation to control what happens to its and its citizens' data. Many nations that have implemented said regulations justify their decision by ensuring that measures were taken to enhance technological sovereignty and security, while not allowing sensitive data to fall into the wrong hands.

On the other hand, data localisation laws have been used by national governments to monitor and manipulate their population, by controlling what data goes through their borders to and from the nation.

When taken to the extremes, data localisation can isolate a nation digitally and physically, providing them with the opposite result of what they may have wanted. By keeping all national data in physical servers inside a country, it becomes harder for said nation to be a part of political alliances, and take part in negotiations, among others. This discourages Less Economically Developed Countries from considering lenient forms of data localisation, out of concern that it may damage their economy.

Thus, the question of whether extreme data localisation regulations have to be implemented to ensure a nation's technological independence is a topic commonly seen in international politics.

To summarise, for countries to maintain their independence in the digital realm, it is important to strike a balance between storing data in local servers and allowing other Member States to view said data.

DEFINITION OF KEY TERMS

Data Localisation

Data localisation or data residency regulations mandate that prior to being transmitted internationally, data regarding inhabitants or residents of a certain country must first be gathered, processed, or kept there.[1]

Normally, the information can only be sent when it complies with regional privacy or data protection regulations, which may include notifying users of its intended purpose and getting their agreement. Extreme Data Localisation, however, describes the state of data localisation, where access to data is either extremely limited or unavailable to persons located outside a nation's borders.

Technological Security/Cybersecurity

Technological security, often known as cybersecurity, is the safeguarding of data and computer systems against loss, theft, and unauthorised access.[2]

Tech Sovereignty

Despite the lack of a formal definition, technological sovereignty can be interpreted as the avoidance of situations in which a country is dependent on a single or small number of foreign suppliers for technologies that are essential for start-ups, as well as for the economy and social well-being.[3]

Less Economically Developed Country (LEDC)

Certain nations, which face financial crises are known as Less Economically Developed Countries (LEDCs). This economic struggle has also led to humanitarian and food crises, in certain nations in the category.[4]

Top-Level Domain

Top-Level Domains (TLDs) are anything a domain name has after the last dot in its web link. Usually, the TLD will be based off of the nation a website operates from (e.g.: ".gr" for Greece, ".kz" for Kazakhstan).[5]

---

[1] Imperva. "Data Localization." Learning Center, www.imperva.com/learn/data-security/data-localization/

[2] The Editors of Encyclopaedia Britannica. "Computer Security | Definition & Facts." Encyclopedia Britannica, 20 July 1998, www.britannica.com/technology/computer-security

[3] "What is Data Sovereignty? | Definition from TechTarget." WhatIs.com, 26 Mar. 2013, whatis.techtarget.com/definition/data-sovereignty

[4] United Nations. "Least Developed Countries (LDCs) | Department of Economic and Social Affairs." Welcome to the United Nations, www.un.org/development/desa/dpad/least-developed-country-category.html

[5] Paruch, Zach. "What Is a Top-Level Domain? TLDs Explained with Examples." Semrush Blog, 3 Feb. 2023, www.semrush.com/blog/top-level-domains/

Digitisation

A process, where a nation or institution stores and handles data digitally. The term also describes the transition of something from the physical to the digital realm.[6]

Surveillance

Surveillance describes the diligent observation of a person, sometimes without their consent, to collect information about their - personal - life. Countries may monitor their citizens to ensure their laws are being followed.[7]

Public Security

Public Safety (or Public Security) is often defined as the protection of the public, i.e. a nation's citizens. Those who uphold Public Safety are called Public Safety Officers, a term which includes services like Fire Departments, Police Departments and Healthcare Institutions.[8]

BACKGROUND INFORMATION

The History of Tech Sovereignty Attempts and Data Localisation

As the Internet and data storage have progressed, the need for more secure methods and regulation of personal data have also become more prevalent. The adoption of data localisation has been rising, with governments worrying that a nation's sovereignty may be at risk if it cannot exert complete control over data held in its boundaries.

Although data localisation practices became prominent in the 21st century, data security - as in the need to securely transport and store data - and the idea of technologically independent nations started with the history of the internet itself.

1980s - Birth of the Internet

The Internet was established on January 1, 1983. As the technology was not yet widely used by the public, the idea of tech sovereignty was less well-known than it is now. Despite this, certain nations were already starting to focus on taking their first steps into the digital world. It is also important to note that nations in the 20th century did not need to implement data localisation to begin this process.

---

[6] Oxford Learner's Dictionaries. "Digitization." Oxford Learner's Dictionaries | Find Definitions, Translations, and Grammar Explanations at Oxford Learner's Dictionaries, www.oxfordlearnersdictionaries.com/definition/english/digitization

[7] Cambridge Dictionary. "Surveillance." Cambridge Dictionary | English Dictionary, Translations & Thesaurus, dictionary.cambridge.org/dictionary/english/surveillance

[8] The Government of Austin, Texas. "What Is Public Safety?" AustinTexas.gov, 24 Mar. 2021, www.austintexas.gov/blog/what-public-safety

China was one of the first nations to undergo modernisation with its "Four Modernisations"[9] programme. Starting in the late 1970s, but continuing until the 1980s, one of the pillars of the programme focused on science and technology, which included what is now the Internet. This was China's early attempt at achieving technological sovereignty and allowing digital content to reach its citizens.

Another example of a nation starting to develop computer networking technology in the 1970s-80s was India. Although it was not as densely populated or financially stable as it is nowadays, the early renditions of computer networks, such as the Advanced Research Projects Agency's (ARPA) computer network (also known as ARPANET), made their way to the Indian Subcontinent.

Experts in the field, like Srinivasan Ramani[10], who was part of the team that created the Internet's precursor in India, known as ERNET, reckon that this early development is crucial in LEDCs as it allows for said nations to switch to newer and more effective technologies easier.

[9]The Editors of Encyclopaedia Britannica. "Four Modernizations." Encyclopedia Britannica, 6 Dec. 2021, www.britannica.com/topic/Four-Modernizations

[10]Source: Ramani, Srinivasan. "The Story of How the Internet Came to India: An Insider's Account." *News18*, 14 Aug. 2015, www.news18.com/news/tech/the-story-of-how-the-internet-came-to-india-an-insiders-account-1039533.html.

Table 1: Dimension Comparison Summary

Dimension or Component	Advantage (C = China, E = Even)
Pervasiveness	
users	C
hosts	C
geographic dispersion	
top-tier political divisions with POPs	C
number of cities with POPs	C
sectoral absorption	
commercial	E
education	C
government	E
health	E
Connectivity infrastructure	
domestic backbone	C
high-speed access	E
exchanges	E
international bandwidth	C
Organizational infrastructure	
telecommunication competition	E
backbone competition	C
access provider competition	C
coordinating organizations	E
Sophistication of use	E

Figure 1: The different sectors used to compare network usage between two countries. The sectors where China held an advantage over India are marked "C" and those where both nations were equal are marked "E".[11]

2000s - Tech Sovereignty and the "Digital Revolution"

The turn of the century marks a phenomenon that could be described as a "Digital Revolution". A transition from traditional means of completing tasks to digital solutions could yield quicker and more effective results.

Though this phenomenon was first documented in the 1990s, its popularity increased greatly in the 21st Century, due to the availability and convenience of computers and other digital systems.

This sudden rise in popularity pushed more nations to seek their digital sovereignty and provide citizens with more Internet-based solutions.

In trying to become digitally independent, national governments feared that how they handled the data of citizens, companies and institutions would be an obstacle to the said goal. By allowing third parties to handle and transmit data,

[11] Press, Larry, et al. "The Internet in India and China." Wayback Machine, 2 Apr. 2003, web.archive.org/web/20030402151332/www.isoc.org/isoc/conferences/inet/99/proceedings/3a/3a_3.htm

there was the concern of misuse, either by being sent to ill-intentioned actors or used as reconnaissance against the state in question.

The above, along with other concerns on privacy, development and control over the internet also led to the idea of data localisation regulations, which state that the data of citizens, companies operating from or companies operating in a specific nation must be stored in servers physically located in the country.

The most infamous example is the US PATRIOT Act[12], which allowed the US government to collect and store data from its citizens in US servers. While not a data localisation policy per se, as the Act did not wholly disallow the above-mentioned data to also be stored overseas, it is viewed as an infringement of the right to privacy, in the name of technological sovereignty and security.

2010s - New Standards for Cybersecurity and the Expansion of Data Localisation Laws

The previous decade proved to be crucial to the Internet's development. The mobile phone became more than just a device. With the rise of social media, the personal data that needs to be stored also grew exponentially. From biographical data (like a person's DOB) to citizens' government files, most types of essential data started to be stored digitally for the convenience of all parties.

Threats to digital security have increased, causing nations with existing cybersecurity and data localisation laws to strengthen them and prompting those without such laws to consider implementing them.

Some of the most prominent examples of data localisation are Kazakhstan's Personal Data Law, and India's amended Information Technology Act in 2013 and 2014, respectively.

2013 marks a crucial year in data security. The National Security Agency (NSA) of the United States was collecting the telephone data of tens of millions of

[12] "USA Patriot Act." *Life and Liberty Archive*, www.justice.gov/archive/ll/archive.htm#:~:text=The%20USA%20PATRIOT%20Act%2C%20enacted,attack%20on%20the%20United%20States.

Americans to ensure the prevention of any illegal activity, according to a story in the Guardian newspaper at the beginning of June 2013.[13]

The NSA, allegedly, also violates privacy rules hundreds of times annually, according to documents that were released to the Washington Post in the middle of August of that year.[14] The aforementioned issues, which had been raised by reputable news agencies citing the findings of Edward Snowden, a former NSA employee, caused the uproar in extreme measures to protect citizens' privacy.

The last major events in this decade take place in 2018, in the European Union (EU). The General Data Protection Regulation (GDPR), passed in May of 2018, outlines how personal data must be handled, including a guideline that prohibits the transfer of data outside the EU's borders, unless the receiving nation agrees to abide by the GDPR.

In November of that same year, however, the EU passed Regulation 2018/1807, which recognises that a regime of data localisation in the European Union may lead to a lack of cooperation between its members.

According to the regulation, data localization, in its current form, stands in the way of the EU's internal market and the free provision of data processing services within its borders. Therefore, data localisation practices need to be outlawed unless they are exempted by EU legislation (i.e. threats to public safety and national security).

2020s - Present Day

In the 3½ years of the 2020s, the countries that have adopted some form of data localisation have reached a historical high. 62 nations had imposed data localisation regimes in 2021, with many more considering a similar course of action. For comparison, in 2017 the number of states with data localisation laws was 35.

[13] "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*, Guardian News and Media, 6 June 2013, www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[14] "NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds." *Washington Post*, 15 Aug. 2013, web.archive.org/web/20130904223528/http://articles.washingtonpost.com/2013-08-15/world/41431831_1_washington-post-national-security-agency-documents.

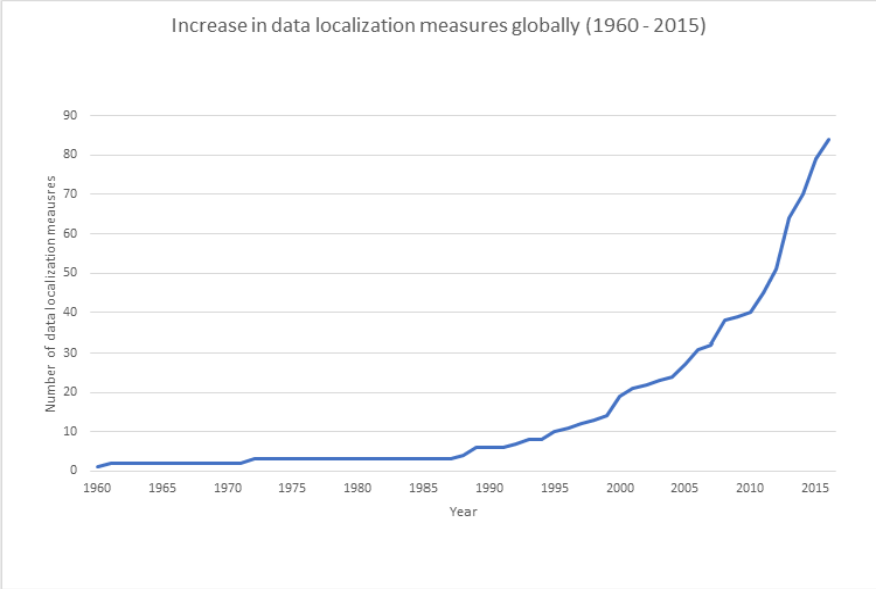

Figure 2: Increase in data localization measures globally (1960 - 2015)[15]

Data localisation has also been used in warfare. After Russia's invasion of Ukraine in February 2022, the Russian Government passed The Federal Law on Personal Data to place stricter and clearer requirements on local and international data operators about how they deal with data, as well as how they comply with this and all other localisation laws.

Causes of Data Localisation

Data localisation differs in form from nation to nation. Though the benefits of this practice that cause nations to implement data localisation regimes are similar in nature. One of the main causes for said policies stems from nations wanting to protect their sovereignty and their citizens. A rising trend of attacks on the sovereignty of certain nations has enabled them to take extreme measures.

Privacy is a catalyst for the implementation of data localisation. As more and more nations concern themselves about the social impact of data privacy (i.e. how society becomes more vulnerable in the case of a lack of privacy), governments enforce this regulation to allow them to control the flow of data.

Finally, a nation may cite financial incentives as the cause for the aforementioned regulation. This level of control requires the appropriate infrastructure, which many nations do not have. Without it, governments who seek to localise their digital activity will need to raise funds, through their citizens and allies, to support modernisation projects of that scale.

[15] Wu, Emily. "Sovereignty and Data Localization." Belfer Center for Science and International Affairs, July 2021, www.belfercenter.org/publication/sovereignty-and-data-localization#footnote-027

The Rise of Extreme Data Localisation

The term "Extreme Data Localisation" describes a localisation regime, where the processing, transfer and access to certain or all types of data in a particular nation must occur in servers physically located in that nation. Lawmakers and Governments tend to adopt extreme forms of data localisation for a variety of reasons, including national security, privacy, financial development and technological security.

The mentioned policies may seem advantageous at first glance, but prove harmful when considering certain factors. If a nation implements these policies, its economy may be affected, significantly reducing trade volume, productivity, and raising costs for businesses that depend on data (i.e. health care).

It is becoming more and more common for nations to assert their data sovereignty by passing these data localization laws, particularly if the nation is not in a strong geopolitical position.

No matter where or by whom the data is held, governments frequently want to exert their authority over it. To tighten control over citizen data, domestic storage places decision-making and access rights inside national boundaries. Additionally, it works against foreign firms in favour of local ones.

Forms of Data Localisation - Case Studies

The regulations governing data localisation differ from one country to another as they are part of their legal system. The examples below are some of the more common variations.

Kazakhstan - Localisation on all websites located in the nation.

Kazakhstan, located in northwest Asia, has implemented data localisation in a very peculiar way. Instead of forcing companies and institutions to store specific types of data on Kazakh servers, the requirement is that all websites registered under a Kazakh Top-Level Domain (.kz) must store all their data locally.

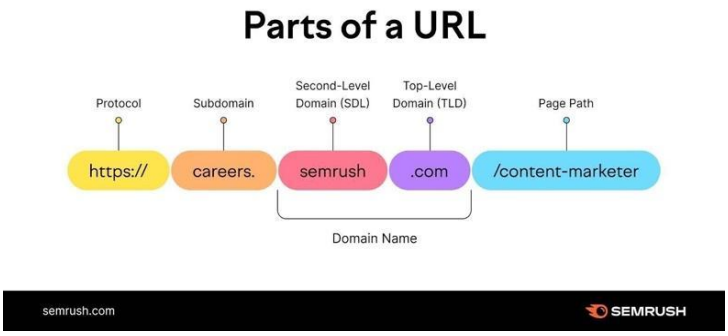

Figure 3: The parts of a Uniform Resource Locator (URL), including the position of the Top-Level Domain (TLD). [16]

All websites require a Top-Level Domain (TLD) to function, which directs the user to the correct location on the Internet. TLDs are also reserved for nations, typically using the country code.

With the above in mind, since most web-pages ending in .kz operate, almost exclusively, from and in the nation, this form of localisation allows a country to exert control over its own "corner" of the Internet. In the case of Kazakhstan this form of data localisation has allowed it to not rely on neighbouring nations to run its web services, but does not isolate it from other countries.

China - Local Access, Transfer and Storage

The most common form of data localisation is found in The People's Republic of China. Vital information infrastructure operators (CIIOs) are required under Article 37 of the "Cybersecurity Law of the People's Republic of China" (CSL) to keep sensitive data created by vital information infrastructure in China.

The "Population and Healthcare Information Management Measures", "Regulation for the Administration of the Map", and "Telecommunications Regulations of the People's Republic of China", among others, extend the types of data to be affected by data localisation to include maps, health/patient data and telephone records.

This means that all data, personal or not, that are considered to be vital to the function of China's products and services are only allowed to be stored, accessed and transferred from servers located in China - and other Chinese Autonomous Regions (i.e. Taiwan, Hong Kong and Macau). The inclusion of Telecom Records in the PRC's localisation laws has raised concern that it is being used to spy on Chinese Citizens, without their consent.

The collection of data in China has raised concern on the privacy of citizens' data, something that data localisation aims to safeguard. The CSL, comparable to the GDPR, has succeeded in protecting Chinese Tech Sovereignty and making the Internet in China a safer space, but it has been criticised for limiting the right to free speech in the nation, by collecting the aforementioned data.

Brazil - Conditional Localisation

Another form of localisation is present in Brazil, where transferring data overseas requires meeting certain requirements.

[16] Paruch, Zach. "What Is a Top-Level Domain? TLDs Explained with Examples." Semrush Blog, 3 Feb. 2023, www.semrush.com/blog/top-level-domains/

International data transfers are only permitted under the General Personal Data Protection Law (LGPD) in certain circumstances, such as when recipient nations guarantee an adequate level of data protection, when authorised legal mechanisms are used (such as contracts ensuring privacy), or when data subjects have given their explicit consent.

According to the regulation, a map of the personal data that businesses gather and handle must also be created and updated. Additionally, organisations must make sure that they are keeping track of data subjects' consents and revocations. This is a practice that should be followed in all cases, even if they are not included in the LGPD in order to demonstrate compliance.

The Brazilian form of data localisation provides a middle ground between local and overseas access, where only certain places can store sensitive data outside Brazil.

India - Local Copies

In India, sensitive personal data, such as financial information, must be maintained in India in accordance with the Personal Data Protection Bill; but, if certain conditions are satisfied, a copy of the data may be sent worldwide.

The government must determine that the receiving nation offers appropriate security. Then, the operator gives their express approval, and the transfer is carried out in accordance with a contract or intra-group plan that has been authorised by the Data Protection Authority. The above transfer can also be expressly permitted by the Data Protection Authority.

United Kingdom - Conditional Transfer and Access, no local copy needed

The approach outlined in the legislation of the United Kingdom allows for the transfer and access of data under certain conditions, without needing a local copy of the aforementioned data. Many Acts have been passed on data privacy and localisation, with those still in effect being the “Data Protection Act 2018” and the “Companies Act 2006”, which protect personal data and data collected by companies, respectively.

Similar to Brazil, the United Kingdom tries to ensure the privacy of its citizens by allowing the transfer of data when the host can ensure that said data will be stored securely.

Mexico - Free flow of Data

The final category in this section encompasses all nations with no known localisation laws. It is important to note, that these countries can still take measures to protect personal data, without needing to implore extreme measures.

In the case of Mexico, the only related regulation passed is the "Federal Law on the Protection of Personal Data Held by the Parties", which does not require local storage nor places requirements on third parties wanting to access, store and handle citizens' data.

Impact of Data Localisation Policies

As data management evolves, data localization policies increasingly impact important sectors of a nation's governance. The four sectors where the impact is most prominent are security, privacy, financial development and tech sovereignty.

National Security

Data localization is a widely implemented measure in cybersecurity legislation, designed to safeguard sensitive information from unauthorised access by various entities, including governments, organisations, and individuals with malicious intent.

While adhering to these regulations can help prevent data breaches, it does not necessarily ensure that authorised parties will have access to the protected data for necessary processing.

Naturally, a nation wanting to protect its sovereignty from opponents can be achieved through data localisation. However, problems arise when "national security" also encompasses the private life of citizens, under the pretence that they too could oppose the state and its government - if not thoroughly checked.

Data Privacy

Data Privacy is the most commonly cited reason behind localisation policies. Technically, by limiting who can access, transfer and modify data, a nation can ensure that no data reaches people or countries who want to harm its citizens. Furthermore, as data breaches have become more common, data privacy is a top priority for governments, as confidential files can also be leaked.

It is not fully confirmed if data localisation can safeguard private data. In recent years there have been multiple scandals, where companies who have access to data sell it - or share it in any way, shape, or form - to gain profit.

The nations concerned with data privacy (e.g. Member States of the EU) implement these measures with good intentions, though said data could be leaked if it is not handled correctly, which would diminish trust in the nation's ability to protect its citizens' privacy.

Financial Development

A nation considering extreme data localisation guidelines must remain careful as well. If a balance is struck between localisation and overseas access, the

nation is set to develop greatly. In the case it chooses to fully localise its data, though, it runs the risk of isolating itself from the digital, international community, thus making financial development in the tech sector more difficult.

Technology has been proved to be a very profitable market in the modern era, with the nations participating in it enjoying a financial bloom. Trying to join this market requires the technological sovereignty of a nation, allowing it to produce and sell tech products and services.

Tech Sovereignty

All of the above lead to the final sector that data localisation impacts is the topic of this guide, namely, tech sovereignty. Compiling all the above, in the case of most lenient localisation regimes, the practice can help safeguard a nation's technological sovereignty. But, the risks of stricter regulations often outweigh the advantages.

Advantages and Disadvantages of Data Localisation

A political agenda of strict data localisation to solidify a nation's sovereignty would have positive and negative consequences. The primary benefits of data localisation policies include ensuring better data privacy and security, creating positions in managing said data, and quicker transport, due to the data not needing to "travel" from overseas servers.

Data localisation, however, often causes more harm than good. Said regulations are said to fail in increasing security, make little contribution to streamlining the regulatory landscape, and inflict economic damage on the economies where they are adopted, making it more difficult for Less Economically Developed Countries (LEDCs) to adopt these policies. Furthermore, data localisation can be a trade barrier, as companies cannot access data from all nations.

To transition away from these practices, other approaches must address the issue of sovereignty loss by balancing local control and overseas storage. For example, a nation could require local copies of data, whilst allowing for overseas storage in nations which fulfil certain criteria (i.e. privacy of data, tech security), thus allowing the nation to be technologically independent.

Implications and Future of Data Localisation

Data localisation practices have evolved greatly in the last decades. With a rise in the awareness towards technological sovereignty, which started almost forty years prior to the 2020s, the world finds itself in a dilemma.

On one hand, citizens and governments believe that data localization ensures safety and independence in the digital world. On the other hand, in extreme scenarios, data

localization can harm a nation's economy or collaboration prospects with other countries or alliances.

The most common reason for the implementation of data localisation is the technological security of the nation affected. In this era of technology, where all data is stored digitally, legislators consider these solutions to ensure that confidential and personal data cannot be accessed by third parties acting.

However, based on some case studies and events mentioned above, it can also be implied that extreme data localisation policies are not solely implemented in the name of tech sovereignty, but can also be used with malicious intent (e.g. spying on citizens).

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

Brazil

The Federative Republic of Brazil, located in South America, is considered one of the most developed countries in the continent. In the digital sector, however, the nation is considered to be lagging behind other nations in similar circumstances.

This situation led academics, researchers and activists to take matters into their own hands. This aforementioned group of intellectuals, believing that Brazil's scientific and technological advancement is hindered by their reliance on overseas firms and organisations, delivered a letter to Luiz Inácio Lula da Silva, the then-presidential candidate for the Workers' Party (the currently ruling party of Brazil) on 16 October 2022 titled "Emergency Program for Digital Sovereignty."

Before that, the only law passed was General Data Protection Law (Federal Law 13709/2018), which only set regulations on data transfer.

China

China is a nation with a rich history in terms of technological advancements. Being the first nation to undergo a process of digital sovereignty, it did not originally have to rely on data localisation to ensure security.

In the current digital landscape, however, the PRC has introduced numerous localisation regulations, in an effort to ensure cybersecurity and protect private data from third parties. Examples include the Population and Healthcare Information Management Measures, Regulation on the Administration of Credit Investigation Industry, and the Telecommunications Regulations of the People’s Republic of China, among others. What these regulations have in common is the inability to transfer data, even under specific conditions as well as strict enforcement from the central government.

The political landscape of the People's Republic of China also influences the measures taken and how they affect its citizens. In recent times, the nation has been accused of using its Cybersecurity Law to monitor its citizens. Through the "Social Credit" System, for example, even model citizens are put under pressure. The nation of China has introduced a localisation and cybersecurity regime, with the purpose of illegal surveillance of its people, in the name of data privacy.

Greece

The Greece 2.0 Plan, a series of regulations, loans and other actions taken by the Mitsotakis administration and the Hellenic Republic to modernise the nation and further its entry in the digital world.

The technological advancement plan includes many measures, such as expanding and supporting the National Telecommunications Network and developing the framework, infrastructure, capacity and capabilities for public data governance, among others which would allow for the nation to be technologically independent.

As a member of the EU, Greece abides by the GDPR and Regulation 2018/1807, which, among other guidelines, includes hosting data in servers located inside the borders of the EU, rather than overseas, while disallowing EU Members from implementing extreme data localisation laws and promoting cooperation, respectively.

Indonesia

The region of South-East Asia contains many nations which have implemented data localisation policies, one of them being Indonesia. The nation is leading in this regard, as the regulations passed encompass multiple aspects of governance, including cybersecurity - as seen in Government Regulation 71 (2019) and Ministerial Regulation no. 20 of 2016, concerning all and public data, respectively.

Indonesia, one of the biggest nations in the area - in terms of landmass - aims to benefit greatly from tech sovereignty, allowing it to reap the benefits of technological independence (i.e. financial improvements). The above would require the nation to provide the needed infrastructure and/or improve its existing infrastructure, with the help of the international community.

Kazakhstan

Kazakhstan, as seen above, has tackled data localisation in a unique way, to achieve tech sovereignty in a geopolitically unfavourable state due to e.g., being a landlocked nation. In this attempt, the Personal Data Law (2011) prohibits all websites ending in .kz, the nation's Top-Level Domain, from storing their data overseas. The regulation would later also encompass personal and national data in an effort to ensure cybersecurity.

In recent times, the nation has undergone major governmental reforms. Although the ruling party (Amanat) still has the majority in the revamped parliament, the newly-

formed opposition could lead to dialogue being used to find solutions that benefit everyone in the nation. Nonetheless, the Personal Data Law is not due for reconsideration in the Kazakh Parliament, although that could change in the months - or years - to come.

Nigeria

According to popular belief, the African Continent is often considered "underdeveloped". This statement may be proven false, seeing the region's development in certain areas of modernisation, even in periods of turmoil. This, in some nations, also translates to data localisation being made law - like in the West African Nation of Nigeria.

The nation, as of date, has introduced two regulations. The first, named Guidelines for Nigerian Content Development in Information and Communication Technology, aims to localise all data in the categories of National and Public Security, as well as Economic Development. Nigeria, through its central bank, has also passed the Guidelines on Point-of-SaleCard Acceptance Services in 2011, which requires the localisation of Point of Sale (POS) data, to allow for safer and easier transactions

Meta, Inc.

Meta, the company owning popular social media platforms Instagram, Facebook and WhatsApp, among others, has been under fire for its lacklustre security of user data. Facebook, specifically, has been the centre of controversy ever since the 2010s, when Cambridge Analytica gathered private data to use in political advertising.

With the introduction of the GDPR, as seen below, Meta has started to adapt their services to follow European protocol. This, however, has not stopped the EU from outlawing Meta's newest product - titled "Threads" - citing privacy concerns.

European Union (EU)

The EU's GDPR policy is a prime example of how data localisation and tech sovereignty can expand to alliances and organisations. By providing EU Members with a common framework, it can be ensured that data that is created in the EU, stays in the EU and is only transferred when the privacy of its citizens is not at risk.

However, the European Union serves a further role in this topic. By passing regulation (2018/1807), the alliance serves as the first example of an entity scaling back data localisation policies. The regulation, essentially, discourages EU Members from implementing data localisation and only abiding by the GDPR, which itself is a more lenient version, focusing on data privacy, rather than local storage and access.

TIMELINE OF EVENTS

DATE	DESCRIPTION OF EVENT
January 1, 1983	Tim Berners-Lee, a British scientist at the European Centre for Nuclear Research (CERN), creates the World Wide Web, which becomes the Internet we know today.
July 1990	ARPANET is discontinued, due to the prominence and abilities of the World Wide Web.
January 1997	China starts developing its technological infrastructure, in order to become less dependent on foreign technology.
October 26, 2001	The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) is passed in the US, which allows the US Government to process and view the data of US citizens and companies that operate from or with the USA.
June 2011	Kazakhstan introduces its first data localisation laws, requiring all local websites (ending in .kz) to store their data in Kazakh servers.
May 20, 2013	According to leaked documents by Edward Snowden, the US government collects surveillance data on its citizens and people globally, causing criticism towards US IT companies and discussions on stricter data localisation regulations.
August 19, 2017	India passes the renewed Information Technology Act, re-establishing the office that controlled data storage, among other measures.
May 23, 2018	The Data Protection Act 2018 is ratified in the United Kingdom, extending the scope of the Companies Act 2006 to personal data.
May 25, 2018	The General Data Protection Regulation is passed and applied in the EU, which aims to protect EU citizens' privacy.
July 13, 2021	The Greek government announces the "Greece 2.0" Project, which -among other reforms- promises the digitalisation and modernisation of the country.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

Economic and Social Council - ECE/CTCS/2023/7 [17]

This note from the United Nations (UN) Secretariat on Integrating digital economy considerations into Studies on Regulatory and Procedural Barriers to Trade covers how the digital age, along with recent healthcare events is affecting global trade.

The Note was drafted in the Economic and Social Council (ECOSOC) and names data localisation as one of the hindrances. To quote: "Other challenges are associated with the lack of consensus on the international regulation of novel issues, such as data privacy and protection, data localization measures, cybersecurity, [...] can lead to divergent approaches at the national level, thus, creating barriers for cross-border digital trade."

The note goes on to propose that in order for trade to resume, data localisation methods should be made more lenient, in terms of data transfer.

Regulation (EU) 2018/1807[18]

The European Parliament and the EU Council agreed a legislative revision abolishing data localisation limitations on November 14, 2018. The Regulation (EU) 2018/1807 became effective in all EU Member States in May 2019.

The rule forbids the storage or processing of non-personal data under localization rules implemented by EU Member States. There is an exception to the general ban in cases when public security justifies data localization requirements.

The regulation does not cancel out the General Data Protection Regulation (GDPR), as the Union still requires personal and private data to be safeguarded.

Sustainable Development Goals (SDGs)

In 2015, the UN proposed the 2030 Agenda for Sustainable Development, a common framework for peace and prosperity for people and the planet, both now and in the future.

The 17 Sustainable Development Goals (SDGs) compose the centre of the agenda. They are the UN's urgent call to action for all nations, both LEDCs and MEDCs, by creating a global partnership in order to eradicate poverty and other forms of

[17] United Nations - ECOSOC. "Integrating digital economy considerations into Studies on Regulatory and Procedural Barriers to Trade." ODS, 17 Apr. 2023, documents-dds-ny.un.org/doc/UNDOC/GEN/G23/081/13/pdf/G2308113.pdf?OpenElement.

[18] European Union (EU). "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." EUR-Lex — Access to European Union Law, 14 Nov. 2018, eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1807

deprivation, policies that enhance health and education, lessen inequality, and promote economic growth, among others.

Out of the 17 Goals, the 8th and 9th Goals are of importance to the topic at hand. As extreme data localisation can stunt economic growth, nations must make decisions with Goal 8 in mind, which focuses on economies and financial recovery.

The 9th Goal, which tackles infrastructural issues, could be adapted to include and better digital infrastructure, allowing for more nations to achieve tech sovereignty.

POSSIBLE SOLUTIONS

Creation of a common framework for nations to decide what types of data have to be stored locally

This solution, which has already been implemented - albeit at a smaller scale, would allow for the easier understanding of regulations by both governments and citizens.

Seeing as the most common issue with data localisation is the balance between local access and overseas cooperation, this framework would allow for all nations to reach a consensus, which they would have to follow, leading to fewer misunderstandings

This common framework would be drafted at an international conference (UN General Assembly, or independent from the UN), where Heads of State/Ministers in charge of digital security and technology would be present. After the proposed document has been signed, it would gradually be implemented by all signatories, by adapting their cybersecurity laws.

Provision of aid to LEDCs, allowing them to achieve Tech Sovereignty

Seeing as tech sovereignty is a matter of importance for developing nations, including LEDCs, the proper financial support could lead to a decline in data localisation practices.

Nations in the process of digitisation could receive help - both financial and infrastructural - to build the needed networks and services, achieving tech sovereignty. In exchange, the nation would be discouraged from adopting data localisation measures, since its sovereignty would not be at risk.

The World Bank, the United Nations, as well as Member States could offer grants - or loans - to act as a financial catalyst for modernisation in LEDCs. In the case of loans, the two parties would also agree on a payment plan for the borrowing nation (i.e. through the implementation of a 10-year repayment plan).

Enhancement of Tech Security between Nations

With national and technological security being cited as one of the most important reasons behind the adoption of data localisation, various measures could be taken to enhance tech security in - and between - nations.

For example, new cybersecurity guidelines could be published; elaborating on each Member State's cybersecurity detriments, if any exist. From that report, companies and other nations could collaborate to ensure tech security in the area, without the need for data localisation.

BIBLIOGRAPHY

Abishev, Gaziz. "Has Kazakhstan Become More Democratic Following Recent Elections?" Carnegie Endowment for International Peace, carnegieendowment.org/politika/89513

Andreeva, Ksenia, et al. "Data Localization Laws: Russian Federation." Morgan Lewis, 22 July 2021, www.morganlewis.com/-/media/files/publication/outside-publication/article/2021/data-localization-laws-russian-federation.pdf

Bosoer, Lucía. "Blogs.eui.eu | 520: Web Server is Returning an Unknown Error." List of Blogs - The EUI Blogs, 26 Oct. 2022, blogs.eui.eu/latin-american-working-group/digital-sovereignty-voices-from-latin-america/

British Broadcasting Corporation (BBC). "Edward Snowden: Leaks That Exposed US Spy Programme." BBC News, 1 July 2013, www.bbc.com/news/world-us-canada-23123964

Cambridge Dictionary. "Surveillance." Cambridge Dictionary | English Dictionary, Translations & Thesaurus, dictionary.cambridge.org/dictionary/english/surveillance

Carney, Matthew. "She's a Model Citizen, but She Can't Hide in China's 'social Credit' System." ABC (Australian Broadcasting Corporation), 31 July 2020, www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278

Central Bank of Nigeria. "GUIDELINES ON POINT OF SALE (POS) CARD ACCEPTANCE SERVICES." Central Bank of Nigeria, 2011, www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20(2).pdf

Centre for Information Policy Leadership (CIPL). "The "Real Life" Harms of Data Localization Policies." Centre for Information Policy Leadership, 29 Mar. 2023, www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf

Chan, Kenddrick, et al. "Against the Grain: The data regulatory regimes of Kazakhstan and Uzbekistan vis-à-vis Russia, China, and Big Tech." LSE Research Online, eprints.lse.ac.uk/117154/1/LSE_IDEAS_against_the_grain.pdf

Cloudflare. "What is a top-level domain?" Cloudflare - The Web Performance & Security Company | Cloudflare, www.cloudflare.com/learning/dns/top-level-domain/

Cory, Nigel, and Luke Dascoli. "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them." Cloudfront, July 2021, d1bcsfjk95uj19.cloudfront.net/sites/default/files/2021-data-localization.pdf

Council of the European Union. "The General Data Protection Regulation." Consilium Europa, 25 May 2018, www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

Cross-Guard. "The History of the Server." Cross-Guard, 19 Oct. 2020, cross-guard.com/company/the-history-of-the-server/

Deloitte. "The China Personal Information Protection Law (PIPL)." Deloitte China, 7 July 2021, www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law.html

Economic and Social Council (ECOSOC). "Steering Committee on Trade Capacity and Standards." United Nations Official Document System (ODS), 27 June 2023, documents-dds-ny.un.org/doc/UNDOC/GEN/G23/081/13/pdf/G2308113.pdf?OpenElement

The Editors of Encyclopaedia Britannica. "Computer Security." Encyclopedia Britannica, 30 Aug. 2022, www.britannica.com/technology/computer-security

---. "Four Modernizations." Encyclopedia Britannica, 6 Dec. 2021, www.britannica.com/topic/Four-Modernizations

European Innovation Council. "Statement on Technological Sovereignty." European Innovation Council, 18 Mar. 2021, eic.ec.europa.eu/system/files/2021-06/Statement%20on%20technological%20sovereignty.pdf

European Union (EU). "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." EUR-Lex — Access to European Union Law — Choose Your Language, 14 Nov. 2018, eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1807

European Union. "General Data Protection Regulation (GDPR) – Official Legal Text." General Data Protection Regulation (GDPR), 2 Sept. 2019, gdpr-info.eu/

---. "The Regulation for the Free Flow of Non-personal Data in the European Union." Government of Poland, 29 May 2019, www.gov.pl/web/digitalization/the-regulation-for-the-free-flow-of-non-personal-data-in-the-european-union

Freedom House. "Kazakhstan: Freedom in the World 2023 Country Report." Freedom House, 8 Mar. 2023, freedomhouse.org/country/kazakhstan/freedom-world/2023

Garrido, Miguelángel V. "(2016.04) “All Your Internet Are Belong to Us”: On Nation States’ Claims of Sovereignty over ICT Architecture and Contents*." Berlin Forum on Global Politics, 30 May 2018, bfogp.org/blog/2016-04-all-your-internet-are-belong-to-us-on-nation-states-claims-of-sovereignty-over-ict-architecture-and-contents/

Gellman, Barton. "NSA broke privacy rules thousands of times per year, audit finds." The Washington Post, 15 Aug. 2013, web.archive.org/web/20130904223528/http://articles.washingtonpost.com/2013-08-15/world/41431831_1_washington-post-national-security-agency-documents

The Government of Austin, Texas. "What Is Public Safety?" AustinTexas.gov, 24 Mar. 2021, www.austintexas.gov/blog/what-public-safety

Government of Greece, and Kyriakos Mitsotakis. "The National Recovery and Resilience Plan (Greece 2.0)." Greece 2.0, 9 June 2023, greece20.gov.gr/en/pillars-and-components/

Government of India. "THE INDIAN INSTITUTES OF INFORMATION TECHNOLOGY ACT, 2014." Major Initiatives | Government of India, Ministry of Education, 9 Dec. 2014, www.education.gov.in/sites/upload_files/mhrd/files/upload_document/iiit_2014.pdf

Government of Kazakhstan. "Kazakhstan - Data Protection Overview." DataGuidance, 7 Aug. 2023, www.dataguidance.com/notes/kazakhstan-data-protection-overview

Government of Russia. "Data protection in Russia." DataGuidance, 27 July 2006, www.dataguidance.com/jurisdiction/russia-0

Government of the United Kingdom. "Companies Act 2006." Legislation.gov.uk, 9 Sept. 2023, www.legislation.gov.uk/ukpga/2006/46/contents

---. "Data Protection Act 2018." Legislation.gov.uk, 23 May 2018, www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Greenwald, Glenn. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." The Guardian, 1 May 2019, www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, Glenn, et al. "Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations." The Guardian, 29 Sept. 2021,

www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Human Rights Watch. "World Report 2023: Rights Trends in Kazakhstan." Human Rights Watch, 20 Jan. 2023, www.hrw.org/world-report/2023/country-chapters/kazakhstan

Isaza, John J., and Hannah Katshir. "Brazil Passes Landmark Privacy Law: The General Law for the Protection of Privacy." American Bar Association, 24 Apr. 2020, www.americanbar.org/groups/business_law/resources/business-law-today/2020-may/brazil-passes-landmark-privacy-law/

Kelion, Leo. "Q&A: NSA's Prism Internet Surveillance Scheme." BBC News, 25 June 2013, www.bbc.com/news/technology-23027764

Laboris, Ius. "The Challenges of 'data Localisation' in Kazakhstan." Lexology, 6 Sept. 2017, www.lexology.com/library/detail.aspx?g=913a103d-6fd3-48d7-bf45-0279848c78b5

Lê, Uyên P. "Data Nationalism." Emory Law Scholarly Commons | Emory University School of Law | Atlanta, GA, 2015, scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1154&context=elj

Manancourt, Vincent, and Melissa Heikkilä. "EU Eyes Tighter Grip on Data in 'tech Sovereignty' Push." POLITICO, 29 Oct. 2020, www.politico.eu/article/in-small-steps-europe-looks-to-tighten-grip-on-data/

Merriam-Webster. "Definition of DIGITALIZATION." Merriam-Webster: America's Most Trusted Dictionary, www.merriam-webster.com/dictionary/digitalization

National Congress of Brazil. "Brazilian General Data Protection Law." DataGuidance, 14 Aug. 2018, www.dataguidance.com/sites/default/files/lgpd_translation.pdf

Paruch, Zach. "What Is a Top-Level Domain? TLDs Explained with Examples." Semrush Blog, 3 Feb. 2023, www.semrush.com/blog/top-level-domains/

Ramani, Srinivasan. "The Story of How the Internet Came to India: An Insider's Account." News18, 14 Aug. 2015, www.news18.com/news/tech/the-story-of-how-the-internet-came-to-india-an-insiders-account-1039533.html

State Council of the People's Rep. of China. "Telecommunications Regulations of the People's Republic of China." China.org.cn - China News, Business, Travel & Language Courses, 25 Sept. 2000, www.china.org.cn/business/laws_regulations/2010-01/20/content_19273945.htm

U.S. Department of Justice (DoJ). "USA PATRIOT Act." U.S. Department of Justice, 26 Oct. 2001, www.justice.gov/archive/ll/archive.htm

United Nations Conference on Trade and Development (UNCTAD). "DIGITAL ECONOMY REPORT 2021 - Annex 2." UNCTAD, 20 Aug. 2021, unctad.org/system/files/official-document/der2021_annex2_en.pdf

United Nations. "Goal 8 | Department of Economic and Social Affairs." Sustainable Development, sdgs.un.org/goals/goal8

---. "Goal 9 | Department of Economic and Social Affairs." Sustainable Development, sdgs.un.org/goals/goal9

---. "Least Developed Countries (LDCs) | Department of Economic and Social Affairs." Welcome to the United Nations, www.un.org/development/desa/dpad/least-developed-country-category.html

Unknown. "What is Data Sovereignty? - Definition from WhatIs.com." WhatIs.com, 26 Mar. 2013, www.techtarget.com/whatis/definition/data-sovereignty

Willis, Richard, and Laura Song. "INSIGHT: Data Localization Poses Challenges for Payments Industry and Innovation." Bloomberg Law News, 20 Dec. 2018, www.news.bloomberglaw.com/privacy-and-data-security/insight-data-localization-poses-challenges-for-payments-industry-and-innovation

Ye, Josh. "Timeline: China's Steps to Control Its Data and Information." Reuters, 9 May 2023, www.reuters.com/world/china/chinas-steps-control-its-data-information-2023-05-09/

MULTIMEDIA RESOURCES

Paruch, Zach. "What Is a Top-Level Domain?" Semrush, 3 Feb. 2023, www.semrush.com/blog/top-level-domains/

Press, Larry, et al. "The Internet in India and China." Wayback Machine, 2 Apr. 2003, web.archive.org/web/20030402151332/www.isoc.org/isoc/conferences/inet/99/proceedings/3a/3a_3.htm

Wu, Emily. "Sovereignty and Data Localization." Belfer Center for Science and International Affairs, July 2021, www.belfercenter.org/publication/sovereignty-and-data-localization#footnote-027