Esin
Attorney
Partnership.

Digital Sovereignty:

New Type of State Power or a Frenemy?

Abstract

Digital sovereignty is one of the contemporary trends for governments to either gain dominance or preserve their positions in the international arena. While offering various attractive benefits from a purely governmental perspective such as fighting against unfair competitive advantages of big tech companies, reinforcing law enforcement and attaining economic objectives, data localization also brings along critical disadvantages such as vulnerabilities in terms of data security and obstacles against innovation, international transactions and provision of services. Policy makers should diligently evaluate the pros and cons of restricting free flow of data in an era of ever-increasing digitalized services so as to mitigate the risks associated with limiting data residency requirements. To this end, security concerns need to be addressed, bilateral or multilateral agreements on globally recognized set of rules should be established, and an international body should be established for proper implementation of the multilaterally accepted set of rules and principles.

Keywords: *data localization, personal data protection, cross-border data transfers, data security*

Dijital Egemenlik: Yeni Bir Erk Türü mü, yoksa Dost Görünümlü Düşman mı?

ÖZ

Dijital egemenlik, hükümetlerin uluslararası arenada egemenlik kazanmaları veya var olan pozisyonlarını korumaları için ortaya çıkan eğilimlerden birisidir. Dijital egemenlik için yapılan çalışmalar büyük teknoloji şirketlerinin rekabet avantajları ile mücadele etmek, kolluk kuvvetlerini gücünü arttırmak ve ekonomik hedeflere ulaşmak gibi devletlerin bakış açısından önemli faydalar sunarken; veri lokalizasyonu, veri güvenliği açısından zafiyetlerin oluşması ve inovasyonun, kıtalararası işlemlerin gerçekleştirilmesi ve hizmetlerin sunulmasının önün engeller koyabilmektedir. Bu nedenle yasa koyucuların, veri lokalizasyonunu risklerini bertaraf etmek adına dijitalleşme çağında verinin serbest akışını kısıtlamanın artılarını ve eksilerini doğru şekilde ortaya koyması gerekmektedir. Bu itibarla, veri güvenliğine ilişkin kaygıların ele alınması; küresel olarak kabul gören prensiplere dayanan ikili ve çok taraflı anlaşmaların yapılması; bu çok taraflı kuralların uygulanmasını sağlamak adına uluslararası bir denetim organı oluşturulması düşünülebilecektir.

Anahtar Sözcükler: *veri lokalizasyonu, kişisel verilerin korunması, verilerin yurt dışına aktarımı, veri güvenliği*

a. Introduction

In today's world where we observe ever-increased data-driven economies, the borders have become almost seamless. Data transfers form one of the most prominent global links not only among numerous firms within the same country, but also across several countries. On the other hand, despite increasing globalization and economic interdependence, a rise in inward-oriented tendencies can also be observed in the field of protection of personal data. As such, some governments are inclined to restrict the free flow of data by introducing legal requirements for data residency. Forced data residency, also known as data localization, refers to an attempt to erect barriers to avoid cross-border data transfers. One of the most compelling reasons for this tendency is the growing concerns for efficient law enforcement, surveillance, detection of irregularities and management of socio-economic dynamics due to the decreasing control of certain governments on the data of millions of people (Sargsyan, 2016). Because one of the most prominent ways to collect data on a global scale is through social media platforms and e-commerce websites operated mainly by big tech companies, governments look for a way to keep the data within their reach by imposing new requirements on companies that both use and produce the data. Such requirements serve the purposes of asserting control over data, known as data sovereignty (Wu, 2021).

Nevertheless, considering the positive outcomes of globalization such as innovations and advanced hi-fi services; there are also counter arguments to data-residency. To find a compromise, decision makers should carefully assess concerns and legitimate claims of not only the proponents who support further data localization and control over the data but also opponents who emphasize the benefits of free flow of data and potential drawbacks of data residency requirements. Reaching a consensus between these two stances requires an in-depth analysis of the advantages and disadvantages of both approaches with an effort to minimize the cons with international cooperation and trust.

This article aims to present approaches toward data localization by reviewing various implementations from different jurisdictions. For this purpose, below we categorize the data residency policies across the world under four main groups, summarize the associated policies and then discuss the arguments for and against regarding data localization practices.

b. Types of Data Localization

Data localization rules adopted by various jurisdictions can be examined under four main categories: (i) no transfer rules; (ii) local copy requirement; (iii) outsourcing restrictions; and (iv) conditional requirements.

No transfer rules are the strictest form of data sovereignty mechanisms that necessitate the storing, transmitting and processing to be at the local level and leaves no room for cross-border data transfers. This mechanism can be observed in China, where critical data infrastructures (CIIOs) are required to store personal data in China (China: Data Localization Requirements, 2020). To elaborate, the Cybersecurity Law (CSL) obliges CIIOs to store personal data and critical data that concerns the national interests of the Chinese government and public. The Personal Information Protection Law (PIPL) and the Measures for Security Assessment of Cross-border Data Transfer introduced certain relaxations — albeit based on vaguely designed provisions — into the data localization requirements, which will be further evaluated in the following sections. Another example falling into the "no transfers" category is Indonesia where Government Regulation No. 82 of 2012 requires electronic system operators, which are entities that provide systems to collect, analyze, store and/or disseminate information electronically as public service, to have their data and recovery centers in Indonesia (Wildana, 2020). Nevertheless, due to the equivocal nature of the definition of "public services" under Indonesian laws, the data localization requirement was imposed very broadly on the electronic system operators until Government Regulation No. 71 shed light on the "public services" in 2019.

Local copy requirement, also known as data mirroring, enables governments to have easier access to data that is allowed to be transferred abroad with the precondition of keeping a local copy. Given the additional costs of maintaining a local copy of the data, this method is considered as a mechanism to indirectly encourage data companies to have data localization (IRSG and DAC Beachcroft LLP Report, 2020). For instance, the Indian government requires a local copy to be stored locally if sensitive personal data will be transferred abroad (Wu, 2021). In detail, in the current form of the Personal Data Protection Bill of India, regardless of whether stored within the country or not, critical personal data is not allowed to leave the country except for extraordinary circumstances. On the other hand, sensitive personal data can be transferred abroad if certain conditions such as the data subject's explicit consent or specific authorization of the Indian Data Protection Authority are met and with the condition that a copy is stored in India (Basu, 2020; the National Law Review, 2022). Sensitive personal data under Indian laws covers not only the special category of personal data in the General Data Protection Regulation (GDPR) (e.g., data regarding health, religion, sexual life) but also financial information of the data subjects (IRSG and DAC Beachcroft LLP Report, 2020). It is important to note that more robust and comprehensive regulations are in sight due to the Joint Parliamentary Committee (JPC) 2019 report on the Personal Data Protection Bill that suggests for the Indian government to bring back the copies of sensitive and critical personal data to India (Chakraborty and Walia, 2022).

Several governments opt to regulate outsourcing activities, which eventually amounts to indirect data localization rules. This type of data localization is often observed in the financial services industry in Türkiye. To elaborate, Turkish banks must maintain their primary (i.e., infrastructure, hardware, software and data and other systems related to banking activities) and secondary (i.e., backup of the primary system) data systems in Türkiye. As part of the outsourcing restrictions, these requirements also apply to outsourced services such as cloud service providers. Similarly, outsourced service providers of the banks in Luxembourg and Switzerland are subject to strict legal rules to ensure the secrecy and security of the data concerned. Further, in Switzerland, cross-border data transfer of non-encrypted data is allowed only upon the prior explicit consent of the data subject (IRSG and DAC Beachcroft LLP Report, 2020). In Luxembourg, companies wishing to outsource services must be authorized by the Commission for Surveillance of the Financial Sector (IRSG and DAC Beachcroft LLP Report, 2020).

Last, in certain countries, cross-border data transfers are allowed only upon fulfillment of certain conditions either by the transferor and/or recipient country. For instance, as per the GDPR, whether personal data can be transferred outside the European Economic Area (EEA) or not is subject to fulfillment of one of the following criteria: (a) recipient country has adequate level of protection for personal data; (b) transfer is based on appropriate safeguards with effective legal remedies; or (c) derogation is allowed based on the specifics of the situation (e.g., consent of the data subject, transfer is necessary for the conclusion or performance of a contract).

c. Arguments on Data Localization

There are various arguments on data localization, both arguing against and/or justifying data localization. One main argument is that it is against the free flow of the internet. On the other hand, some argue that establishing data localization mechanisms will not provide the benefits the governments are aiming to have and will cause side effects along the way. Below, we will review and discuss these adverse opinions.

Data localization does not ensure data security

Physical location of data does not guarantee data security. With tendencies toward cloud computing, we are now aware that determining the physical location of data does not necessarily result in ensuring its safety. In fact, gathering data in a single location increases safety concerns. As most of the data protection regulations stipulate the technical and organizational measures that must be taken by the data controllers to ensure security of the data, regulations often tend to fall behind cybercrimes. Furthermore, gathering all data in one place, without backup, would also increase its vulnerability. To mitigate this risk, in cloud systems, depending on the service one chose, data is distributed among multiple servers rather than being stored in a single location (Wu, 2021).

Data localization does not prevent foreign surveillance and may lead to government surveillance

The availability of data to law enforcement agencies is a controversial topic. Governments try to make the data available to domestic law enforcement agencies in order to establish an effective system for detecting crimes and evidence gathering while at the same time trying to protect the data from foreign law enforcement agencies to prevent surveillance. However, such availability may not provide the outcomes that the governments are trying to achieve and also may cause domestic surveillance. The relationship between data localization and law enforcement can be analyzed under two main categories: data availability to domestic law enforcement agencies and foreign law enforcement agencies.

Data availability to domestic law enforcement agencies

When data is stored in a specific country, it allows public authorities, law enforcement and intelligence agencies to access the data, especially for the purpose of preventing and responding to public emergencies. Data localization is an important tool especially for evidence gathering, identifying and prosecuting criminal convictions (Hill, 2014). This aspect eases the prosecutorial process for the crimes that require access to the information stored in other jurisdictions. The disclosure of information from one jurisdiction to another often requires a long process as the authorities may not be very cooperative or the rules between the countries on data disclosure require rather a slow procedure. Therefore, it is argued that storing data domestically reduces the time for evidence gathering, even making it possible to gather evidence for same cases, and increases the effectiveness of prosecutorial and criminal proceedings.

However, this aspect should also be controlled by supervisory authorities as it may easily lead to domestic surveillance. This risk is more evident for countries with legal systems that do not offer the required protection. Storing data locally may make the companies more vulnerable to illegitimate data access requests and surveillance demands and, eventually, may risk the safety and privacy of data subjects (Sargsyan, 2016). Furthermore, domestic surveillance can pose an alarming threat to the fundamental rights and freedoms in authoritarian countries, in particular.

Data availability to foreign law enforcement agencies

The availability of data to foreign authorities brings data security concerns along with a foreign surveillance risk. The invalidation of EU-US Privacy Shield is an example of the approach to prevent access to the data by foreign countries. The EU-US Privacy Shield was invalidated by the decision of the European Court of Justice with its decision dated July 2020 significantly affecting the data transfer between the EU and the US. The European Court of Justice evaluated that in the cases where there is a local surveillance risk in the recipient country that prevents the implementation of GDPR, such transfer constitutes an unlawful data transfer. The decision demonstrates the EU's concern to protect the data of its citizens from the surveillance risk of other countries, especially the US.

However, some scholars argue that the threshold for requesting access to data stored abroad may be lower than requesting access to data stored domestically. For instance, the US laws put stricter thresholds on the collection of data stored in the US, while the use of data obtained from abroad is permissible regardless of the legitimacy of its collection, if there is a "national security interest," which can be interpreted rather broadly (Hill, 2014). Furthermore, as per the US Cloud Act, US based technology companies must disclose the requested data regardless of where the company stores the data (Wu, 2021). Accordingly, the companies that are subject to the US Cloud Act cannot prevent US surveillance by locating their servers elsewhere. Given the above, data localization may not always be very effective to prevent foreign surveillance.

As can be seen, the availability of data to law enforcement agencies may be beneficial for the prosecutorial process but at the same time may trigger both domestic and foreign surveillance risks. Therefore, it is quite volatile whether data localization is the answer to law enforcement agencies' information disclosure requests. A suggested solution would be the efficient use of the mutual legal assistance treaties (MLATs), which may provide the governments with access to information that is stored abroad while also protecting the rights of the individuals. This approach has also been recognized by the International Chamber of Commerce and the European Commission, as the use of MLATs has a higher chance to create an efficient and established system for information gathering (Chander, 2014).

Data localization does not stimulate the domestic economy, on the contrary, it causes harm

The financial effects of data localization are also subject to different arguments. For instance, some scholars argue that it is important to make use of the data domestically to have a comparative advantage on the international era. However, such localization requirements may have side effects, such as leading some companies to leave the market rather than localizing their operations or reducing the contribution of data flow to a country.

Financial benefits

With the technological developments, the significance of data is undeniable. Access to data provides financial and competitive advantage to the companies that can make use of it. Therefore, keeping data within the borders allows local companies to use the data for commercial purposes while leaving foreign companies at a disadvantage. This is especially valuable for the countries with larger markets of consumer groups, such as India and China.

The aim for protecting the domestic economy by implementing data localization requirements also brings a taxation burden against the companies that use data for their operations. For instance, in India, as per the International Tax Law, to impose taxes on a company, the company must have a permanent establishment in India. For the purposes of taxation, having local servers in India may be regarded as having a physical presence in India and, accordingly, such companies may be subject to taxes ("Data Localisation & Tax Impact," 2018).

Financial losses

There are financial side effects of data localization that can be visible from various examples. For instance, a financial technology company operating online payment systems left the Turkish market rather than localizing their systems ("Data Localisation & Tax Impact," 2018).

Moreover, cross-border data flows provide a significant financial contribution to countries, for different sectors. The report of Frontier Economics "The Value of Cross-Border Data Flows to Europe: Risks and Opportunities" indicates that when the EU cannot rely on transfer mechanisms under the GDPR and the countries increase their data transfer restrictions, that would lead to a reduction of EU exports by 4%, which would amount to a 1% reduction on GDP per year. This loss would amount to EUR 1.3 trillion (Mine & Bonefeld-Dahi, 2021). According to this study, the long-term financial effects of data localization must be clearly assessed to see the full picture on its advantages and disadvantages.

Another justification is that data localization leads to the establishment of local servers, which provides a new business area and boosts employment. However, data servers require various technological components but a significantly reduced workforce. The technology is mainly imported into countries by limited suppliers (Chander, 2014). Therefore, the anticipation of governments on its boost to the economy is rather generous than the actual framework.

Data localization increases data sovereignty

As the importance of data increases over the years, it is significant for countries to gain control over the data for economic, technological and governmental purposes. Data localization introduces a mechanism to accomplish this by providing access to data in jurisdictional territories and allowing decision making domestically (Wu, 2021). Establishing data sovereignty holds importance mostly for less developed or developing countries. As per the "Internet & Jurisdiction Global Status Report" (2019), the approach of developing and smaller countries is shaped around the arguments that (i) they do not have a say regarding the internet and its regulations in the international arena and (ii) they have difficulties in enforcing their laws (Khushbu, 2021). Accordingly, the fear of foreign surveillance is more tangible for disempowered countries and the possibility for their law enforcement is lower. This leads them to establish data localization requirements to ensure their data sovereignty. The fear of foreign surveillance does not only affect smaller countries. Developed countries such as the US, China or Russia are also affected by foreign surveillance risks as data is strategically important for these countries to keep/increase their positions globally. Therefore, the strategic importance of data encourages states to introduce regulations to ensure data sovereignty.

While establishing data sovereignty is important, this aspect may be used by governments to increase their control over the data and also the internet. The aim to increase sovereignty together with the aforementioned justifications may be used by governments to justify their aim of gaining control over the private sector, especially the US-based social media and internet companies. For instance, the data localization requirements introduced by several countries, such as Russia, may interfere with the personal rights of data subjects such as freedom of speech and the right to receive information. This may find its best application in the operation of social media companies, as control over these companies allows the blocking of giving and receiving information and, in turn, may lead to censorship (Chander, 2014).

Data localization in Türkiye

In Türkiye, the main piece of legislation regulating international data flows is Law No. 6698 on Protection of Personal Data (**"Law No. 6698"**). Law No. 6698 sets forth four mechanisms for the cross-border transfer of personal data: (i) obtaining explicit consent from the data subject; (ii) meeting the criteria of adequate protection in the target country; (iii) execution of a commitment and obtaining the Turkish Data Protection Authority's (DPA) approval; and (iv) execution of Binding Corporate Rules and obtaining the DPA's approval. The DPA has not published the list of countries that offer adequate protection and the numbers of approved commitments are very limited. Therefore, in practice, most of the companies rely on the explicit consent of the data subjects for the transfer of personal data abroad. Similarly, as per Law No. 5809 on Electronic Communications, traffic data and location data can be transferred abroad only based on fulfilling the notice requirement and explicit consent. As for data localization, the requirements under Turkish law are mainly sector specific. The sectors that establish a data localization mechanism include banking, communications and the internet.

In 2019, with Presidential Circular No. 2019/12 on Information and Communication Security Measures, Türkiye required critical data, such as genetic, biometric, communications and health data, to be stored in Türkiye and introduced the prohibition of procuring cloud services from non-domestic companies for the storage of public institutions' and organizations' data.

The data localization requirements in the banking sector are more comprehensive as they introduce data localization requirements to (i) banks, (ii) internet-based payment service providers, (iii) publicly traded firms and (iv) financial leasing, factoring and financing companies. As per the Regulation on the Bank's Information Systems and Electronic Banking Services, banks need to keep their primary and secondary systems in Türkiye. The primary systems are digital systems, consisting of infrastructure, hardware, software and data that enables the recording and use of the information necessary for the fulfillment of the banks' duties. Secondary systems are the backups of the primary systems that can be used in case of an interruption in the primary systems.

As per Law No. 6493 on Payments and Security Settlement Systems, Payment Services and Electronic Money Institutions, the internet-based

payment service platforms need to store their data in Türkiye for 10 years. The systems and the backup of these systems must be in Türkiye as well. The secondary legislation also sets forth principals on data localization, especially for sensitive customer data. The payment service providers are obliged to keep and store sensitive personal data in Türkiye, if the conditions under the secondary legislation are fulfilled. Furthermore, the data obtained within the scope of the services of payment service providers cannot be shared with or transferred to third parties in or outside Türkiye without a request or instruction from the customer. In addition, as per Communiqué No. VII-128.9 on the Management of the Information Systems, the publicly traded firms must store their primary and secondary systems in Türkiye as well. Similar requirements are also applicable for financial leasing, factoring and financing companies.

As for the communications sector, there are two decisions of the Information Technologies and Communication Board on data localization: eCall and eSIM decisions. The eCall decision regulates the 112-based in-vehicle emergency call systems and requires servers of the communication systems that are onboard vehicles, which enable the rendering of value-added services in addition to eCall, to be kept and located in Türkiye, and the personal data on the system not to be transferred abroad without the express consent of the data subject. The eSIM decision No. 2019/DK-TED/53 (12 February 2019) requires all data generated by eSIM technologies to be kept in Türkiye.

Furthermore, Law No. 5651 on the Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts requires the social network providers that have more than 1 million users to keep the personal data of Turkish citizens in Türkiye.

d. Practices around the World

Russia

Russia is one of the countries that has strict data localization requirements. Russian Federal Law No. 242 requires internet intermediaries to store user data in Russia. The data can be remotely accessed and after the initial collection, the data can be transferred abroad within the limits of data transfer conditions. In 2019, the Russian Federal Security Service (FSB) ordered companies to use equipment that gives the FSB access to detect communications (Cory and Dascoli, 2021).

With the Yarovaya amendments, the telecommunication companies and certain internet companies are required to store copies of communications in Russia for up to three years and to hand them over to the authorities upon request (Cory & Dascoli, 2021). In 2021, Russia further required social media companies to store their data in Russia, similar to requirement set forth under Law on the Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts No. 5651 in Türkiye. As most of these data localization requirements lack judicial oversight, one might argue that data localization is used to monitor the citizens and control their activity by the government.

Similar to Türkiye, the financial institutions are required to keep their primary and backup systems in Russia and the credit institutions are required to keep their electronic databases within Russia. Moreover, recent Russian amendments to Federal Law on Personal Data have introduced new pre-transfer requirements for cross-border data transfers. Namely, the entities are required to notify the supervisory communication authority of their intention for the cross-border data transfer before the transfer and also to conduct an assessment regarding the transfer to ensure security of the data (Anonymous, 2022).

EU

In the EU, personal data can flow freely within EEA and additional data transfer mechanisms are regulated under the GDPR. These mechanisms include Binding Corporate Rules, Standard Contractual Clauses and adequacy decisions.

As for the nonpersonal data, Directive 2018/1807 promotes the free flow of nonpersonal data within EU countries and prevents the member states from establishing data localization requirements for nonpersonal data unless it is justified on the grounds of public security.

On a national basis, for instance as per the German Telecommunications Act, the telecommunication providers are required to store phone numbers and communication details for up to 10 weeks on German servers. Germany is one of the countries that tend to increase data localization by the involvement of telecom companies (Hill, 2014). The largest German telecom company sets campaigns that allows email correspondences to be kept in Germany and new a routing model that allows sending data between two German citizens without having the data leave Germany (i.e., without the involvement of non-EU countries, especially the US) (Hill, 2014). Furthermore, France and Germany also aligned to create a European cloud system called GAIA-X, to increase the digital sovereignty of the EU and to hinder reliance on US-based servers (Cory and Dascoli, 2021).

As can be seen from the initiatives and the regulations in the EU, EU countries encourage the free flow of data within the EU while trying to increase their data sovereignty, with the aim of protecting their citizens' data from other countries' surveillance and decrease the dominance of the US in digital sectors.

China

As one of the most prominent countries when it comes to data localization, China does not have a standalone set of rules that regulate cross-border data transfers and restrictions to reinforce data sovereignty. Provisions on data localization are scattered in various regulations such as the Data Security Law (DSL), which took effect in September 2021, the PIPL, which took effect in November 2021, the CSL and sector-based regulations. The main provision with respect to strict data localization rules stems from the CSL, which includes a very vague and broad group defined as the CIIOs, these are prohibited from cross-border data transfers due to the nature of the data they process (IRSG and DAC Beachcroft LLP Report, 2020). To elaborate, CIIOs collect and process crucial data that is associated with concepts such as public interest, national security and fiscal policies. Additionally, the Chinese Cyberspace Administration brings outsourcing restrictions to CIIOs for using network products and services (e.g., database network, related software and hardware including cloud computing services). Procurement of such products and services is subject to the permission of the Cyberspace Administration.

Recently, the Chinese government introduced some flexibility to cross-border data transfers. According to new regulations, personal data can

be transferred abroad if one of the four criteria set forth under Article 38 of the PIPL is met (PIPL Translation, 2022). Regardless of the mechanism employed, data subject's consent and a personal data impact assessment will be required for cross-border data transfers (Creemers, 2021). For personal data requests presented by foreign judicial and law enforcement authorities, the PIPL further requires approval of the competent Chinese authority. Very recently, the Chinese Cyberspace Administration published the Measures for Security Assessment of Cross-border Data Transfer that introduce additional obligations on large-scale companies for exporting data from China. Accordingly, data transfers that meet certain thresholds such as export of crucial data and transfers by CIIOs or other entities that process more than one million individuals' personal data are now subject to security assessment to be conducted by the Cyberspace Administration (Ho & Zhu, 2022). Given the ambiguous scope of foreign judicial and enforcement authorities and increased costs, paperwork and scrutiny of the Cyberspace Administration, one can argue that the Chinese government would like to reserve its right to interfere in cross-border data transfers on several grounds by way of the vague and broadly interpretable wordings embraced throughout local legislation and complicating compliance.

US

Personal data can almost be deemed as a form of global currency. Given its pioneering position within multinational technology companies and emerging technologies such as AI and cloud computing (Wu, 2021), the US is already at an advantage due to its control over data through geopolitical power assertions.

The US has long been in favor of international cooperation when it comes to sharing information, hence, cross-border data transfers. Indeed, the supportive US approach to data transfers can be clearly observed from diplomatic steps taken by the US government such as the 2020 joint statement between Singapore and the US on the importance of international data transfers in financial services (US Department of the Treasury, 2020). The statement includes clear manifestation of disadvantages about data localization requirements such as increased cybersecurity risks and hindering smooth provision of financial services. Nevertheless, due to the increasing cross-border data transfer restrictions imposed by other countries, the US seems to review its stance against data localization. According to the Center for Strategic and International Studies (CSIS) 2021 report, the US is on the way to issue data localization policies as a result of the pressures from allies and businesses (Ramos, Sheppard and Yayboke, 2021). Currently, the US government aims to ensure the free flow of personal data across countries against the data localization mandates of various countries through international organizations and safeguard provisions in trade agreements such as the US-Mexico-Canada Agreement.

Most recently, to address the situation of uncertainty created regarding data flows from the EU to the US due to the invalidation of the Privacy Shield, on 25 March 2022, US President Joe Biden and European Commission President Ursula von der Leyen announced that the two parties have reached a new transatlantic data transfer agreement. As per the new arrangement, the US will have to ensure compliance with the limitations on signal surveillance and establish a redress mechanism. The US and the EU have reached the agreement "in principle" and the arrangement still needs to be legally adopted. The new arrangement is expected to promote cooperation and digital economic growth between the US and the EU (Bracy, 2022).

e. Conclusion

In the conjuncture at hand, digital sovereignty became the fuel for a new race where governments strive for either gaining dominance or preserving their positions. The main determinant of this competition is the control over data. While offering various attractive benefits from a purely governmental perspective such as fighting against unfair competitive advantages of big tech companies, reinforcing law enforcement and attaining economic objectives, data localization also brings along critical disadvantages on a broader scale. Opponents of restricting the free flow of data are skeptical about the benefits of localization rules in the name of data security by arguing the possibility of vulnerabilities in a country's systems. Additionally, it is claimed that restraining data flows across countries can possibly turn out to be an obstacle against innovation, international transactions and provision of services. Hence, increasing the importance of data for data-driven big tech companies and their users vis-à-vis governments' pursuit of control, surveillance and fear of data-based neocolonialism lies at the heart of this dilemma.

It goes without saying that both sides of the argument should be taken into account by all the stakeholders in policy making. Indeed, proponents of restrictions should consider the benefits that come with the free flow of data such as interoperable financial transactions and communication networks and reduced costs (Sargsyan, 2016). In the same way, one cannot overlook the governments' legitimate need to access data so as to ensure law enforcement.

Therefore, stakeholders should swiftly adopt a solution-oriented approach and focus on objective and enforceable solutions where legitimate interests of both positions are balanced to the utmost. To this end, first, security concerns on which not only justifications but also counterarguments of data localization can be built, need to be addressed. When it comes to protection of personal data, it can be claimed that a universal set of rules and general principles can be applicable to determine the necessary measures to be taken to ensure data security. Hence, bilateral or multilateral agreements on globally recognized set of rules would reassure the stakeholders about data concerns. Second, the terms and conditions of the governments' access to data in other jurisdictions should be mutually agreed on the basis of proportionality and justifiability. Such agreements require international cooperation and mutual recognition of the delicate balance between people's right to privacy and legitimate governmental interests (e.g., public good and national security). Last an international body should be established so as to ensure the proper implementation of the multilaterally accepted set of rules and principles on the cross-border data transfers. Hence, decision makers should diligently evaluate the pros and cons of restricting the free flow of data in an era of ever-increasing digitalized services so as to mitigate the risks associated with limiting data residency requirements.

References

Anonymous (December 2018). Data Localisation & Tax Impact. Financial Chronicle. DOI: https://www.mydigitalfc.com/editorial/data-localisation-tax-impact.

Anonymous (February 2020). United States – Singapore Joint Statement on Financial Services Data Connectivity. US Department of the Treasury. Retrieved from https://home.treasury.gov/news/press-releases/sm899.

Anonymous (July 2022). Russia: Amendments to Law on Personal Data published in Official Gazette. Data Guidance. Retrieved from https://www.dataguidance.com/news/russia-amendments-law-personal-data-published-official#:~:text=266%2DFZ%20on%20Amending%20the,of%2027%20July%202006%20No.

Anonymous (June 2016). PayPal Is Shutting down in Turkey. Insider Intelligence. Retrieved from https://www.businessinsider.com/paypal-is-shutting-down-in-turkey-2016-6.

Basu, A. (February 2020). The Retreat of the Data Localization Brigade: India, Indonesia, and Vietnam. The Diplomat. Retrieved from http://www.viet-studies.net/kinhte/DataLocalizatinRetreat_Diplomat.pdf.

Bonefeld-Dahi, C., Mine, H. (June 2021). The Value of Cross-border Data Flows to Europe: Risk and Opportunities. Frontier Economics. Retrieved from https://www.digitaleurope.org/wp/wp-content/uploads/2021/06/Frontier-DIGITALEUROPE_The-value-of-cross-border-data-flows-to-Europe_Risks-and-opportunities.pdf.

Bracy, Jedidiah (March 2022). EU, US agree 'in principle' to new trans-Atlantic data agreement. Retrieved from https://iapp.org/news/a/eu-us-agree-in-principle-to-new-transatlantic-data-agreement/.

Cory, N., Dascoli L. (July 2021). How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Information Technology and Innovation Foundation. Retrieved from https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

Creemers, Rogier and Webster, Graham (August 2021). Translation: Personal Information Protection Law of the People's Republic of China - Effective Nov. 1, 2021. DigiChina. Retrieved from https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021.

Creemers, Rogier (November 2021). China's Emerging Data Protection Framework (November 16, 2021). Retrieved from https://ssrn.com/abstract=3964684 or http://dx.doi.org/10.2139/ssrn.3964684.

Wildana, Faiq (June 2020). Analysis of The Impact of Data Localization Regulation: Case of Indonesia, Master of Science (Digital Society) Thesis.

Hill, Jonah (May 2014), The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders. The Hague Institute for Global Justice, Conference on the Future of Cyber Governance. Retrieved from: https://ssrn.com/abstract=2430275 or http://dx.doi.org/10.2139/ssrn.2430275.

Ho, D., Zhu, M. (August 2022), China Cross-Border Data Transfer Mechanism and Its Implications, August 2022. The IAPP. Retrieved from https://iapp.org/news/a/china-cross-border-data-transfer-mechanism-and-its-implications/.

IRSG and DAC Beachcroft LLP Report (December 2020) "How the Trend towards Data Localisation Is Impacting the Financial Services Sector". Retrieved from https://www.irsg.co.uk/publications/irsg-report-how-the-trend-towards-data-localisation-is-impacting-the-financial-services-sector/#:~:text=The%20financial%20services%20sector%20is,implementing%20restrictions%20on%20its%20transfer.

Jain, K. (December 2021). Data Localisation: Which Way Is the World Headed? Sunday Guardian Live. Retrieved from https://www.sundayguardianlive.com/legally-speaking/data-localisation-way-world-headed.

Kurth, H. Andrew (January 2022). India's Draft Data Protection Bill Moves Closer to Passage. The National Law Review Vol. XII, Number 6.

Lindsey R. Sheppard, Erol Yayboke, and Carolina G. Ramos (July 2021). The Real National Security Concerns over Data Localization. Center for Strategic and International Studies.

Ramos, C. G., Sheppard, L. R., Yayboke, E. (July 2021). The Real National Security Concerns over Data Localization. Center for Strategic & International Studies. Retrieved from https://www.csis.org/analysis/real-national-security-concerns-over-data-localization.

Sargsyan, T. (2016). Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security. International Journal of Communication, 10, 17, 2221–2237.

Chakraborty, Supratim, and Walia, Harsh. What Does India's Data Protection Bill, 2021 Mean for Foreign Businesses? Lexology.

US Department of the Treasury (February 2020). United States – Singapore Joint Statement on Financial Services Data Connectivity. Retrieved from: https://home.treasury.gov/news/press-releases/sm899.

Wu, E. (July 2021). Sovereignty and Data Localization. Harvard Kennedy School Belfer Center Cyber Project. Retrieved from https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf.

Zhang D. (July 2020). China: Data localisation requirements. Data Guidance. Retrieved from https://www.dataguidance.com/opinion/china-data-localisation-requirements.

Authors

Can Sözer
Partner
CIPP/E
T: +90 530 555 39 63
can.sozer@esin.av.tr

Ecem Elver
Senior Associate
T: +90 530 555 39 74
ecem.elver@esin.av.tr

Gizem Nur Yıldırım
Associate
T: +90 549 439 02 06
gizem.yildirim@esin.av.tr

Ecenur Etiler
Associate
T: +90 549 439 01 93
ecenur.etiler@esin.av.tr