PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

POLICY PAPER

NO. 22 (208), DECEMBER 2021 © PISM

Editors: Sławomir Dębski, Patrycja Sasnal, Wojciech Lorenz

Digital Protectionism: Data Localisation

Oskar Szydłowski

In recent years, under the pretext of protecting national security and citizens' privacy, states have introduced several protectionist measures concerning digital data. The main one is data localisation law, which requires data to be stored and processed in a specific country. In practice, it often serves authoritarian governments in gaining greater oversight of citizens through unrestricted access to and control over data. Furthermore, it has a negative impact on the global economy, especially international trade. The challenge remains to develop regulation at a global level in place of incompatible local regimes.

Data localisation law imposes geographical restrictions on the processing and storage of data. It is the digital form of another protectionist measure—local content requirements, specifying how much of a product must be produced or purchased domestically. There are two types of data localisation: soft, in which a copy of the data, constantly updated, must be located in the country; and hard, prohibiting the processing of data outside the country and thus preventing its transfer across borders. Such law mainly concerns personal and commercial data produced in a given country, and therefore targets companies that process such data, namely large online platforms. The vast majority of this kind of regulation is limited to "data at rest" (inactive, stored data), as opposed to "data in motion" (data that is being transferred, e.g., from one server to another), the restriction of which would require significant changes to the technical infrastructure of the internet.

Data Localisation Laws Worldwide

Measures to limit access to data and enhance data localisation, have gained popularity in the second decade of the 21st century, and particularly since the Arab Spring (2010-2012) and the revelation by Edward Snowden in 2013 of the global scale of surveillance by U.S. services.

Measures to limit access to data and enhance data protection, such as data localisation, have gained popularity in the second decade of the 21st century, and particularly since the Arab Spring (2010-2012) and the revelation by Edward Snowden in 2013 of the global scale of surveillance by U.S. services. In recent years, more than 70 countries have updated existing law or introduced new legislation in this area.

Three approaches to data localisation used by states can be distinguished: open, restrictive, and hybrid. These most often coincide with countries' attitudes towards globalisation, trade barriers, and international cooperation. The open (liberal) approach is characterised by minimal restrictions on data processing, storage, and unrestricted international data flows. This position is represented by the U.S., the UK, Japan, and New Zealand. This does not mean that data privacy is not protected there or that all data can cross borders. The restrictions applied by these countries are minimal and concern, for example, medical or military data.

The most restrictive approach implements a hard data localisation law, often reinforced by other regulations extending the restrictions to data in motion. This policy is pursued by China, Russia, Indonesia, and Nigeria. Russia introduced data localisation in 2015 (Federal Law number 242, further tightened in 2019) and China in 2017 (Cyber Security Law). Both countries, furthermore, plan to expand restrictions on internet service providers in order to centralise and increase control over the internet in the country. Some action in this area has already been taken as a result of the so-called Sovereign Internet Law in Russia and the Network Data Security Management Regulation in China. These measures represent significant interference in the technical sphere of the global functioning of the internet. As a result of the introduced regulations, some companies withdrew their services from the markets of both countries. Those that, according to the regulators, did not comply with the new rules, were banned, such as LinkedIn in Russia.

Hybrid approaches assume only basic geographical restrictions on data, most often in the form of soft localisation. Countries that have relaxed their initially restrictive localisation laws, such as India or Vietnam, also fall into this category. The European Union is a distinct case, putting a very high emphasis on data privacy. This is achieved through the General Data Protection Regulation (GDPR), which regulates the processing of data within the EU, allowing transfer abroad only to countries and organisations that have data protection policies that comply with EU regulations. The GDPR does not explicitly refer to the localisation of data, but, in practice, it restricts the export of data, as access to

The GDPR does not explicitly refer to the localisation of data, but, in practice, it restricts the export of data, as access to data outside the EU is also treated as an international transfer.

data outside the EU is also treated as an international transfer.

Privacy and National Security

The two main arguments used by governments to introduce data localisation laws relate to data privacy and national security. Basically, both argue for limiting access to data, especially for foreign entities. Data localisation does indeed limit this access, but only in the case of hard localisation preventing international data transfers. Otherwise, a continuously updated copy of the data can be stored beyond national borders. Instead, data localisation facilitates access by state apparatus (including special services and law enforcement) in the country where it is located, allowing the development of digital authoritarianism based on mass surveillance and censorship. This poses a significant threat to democracy and human rights, such as the right to freedom of expression or access to information about the actions of authorities.

The geographical location of data has no direct impact on its security. Data localisation laws can even be detrimental for national security because, as a consequence of this regulation, the number of centres storing data increases, making them more vulnerable to attack. Moreover, not all countries have the infrastructure or human resources to ensure an adequate security standard for national data centres. In addition, the more different data localisation regimes exist internationally, the more difficult it becomes for data to be shared by, for example, intelligence services of different countries or international institutions. It also leads to reduced international cooperation and the functioning of states in separate digital networks with limited information flow from the outside world, which increases their isolation and makes diplomatic action more difficult.

Economic Consequences

Data is becoming a key driver of global economic growth, and this dependence will grow with the processes of digitisation and automation. The acceleration is already visible as a consequence of the COVID-19 pandemic, when internet traffic increased by tens of percent year-on-year and many services, including public services, were moved to the digital realm. The added value of data flows between borders alone was estimated at $ 2.8 trillion in 2014. For the EU, estimates point to €3 trillion in added value from foreign data transfers, not including intra-EU transfers, in 2030.

The localisation of data significantly reduces the ability of data to flow across borders. This drastically increases—for both soft and hard localisation—the cost of doing business, especially internationally. The cost of maintaining and updating copies of data can be an entry barrier into particular markets. This is most relevant for small and medium-sized enterprises or for companies planning to expand internationally. As a result, competitiveness and innovation in the economy are hampered, and supranational corporations are favoured, which are likely to pass on the higher costs of hosting and other services to consumers. Data localisation as a protectionist measure, while limiting competition from outside, at the same time closes citizens' access to foreign services that may be cheaper or whose equivalents are not available in the domestic market. Research by consultancy Frontier Economics on behalf of the European Commission (EC) estimates losses of €2 trillion and up to 2 million jobs by the end of the Digital Decade (2030) if international data flows are not liberalised. More than half of the losses incurred are expected to be due to data localisation by the EU itself.

Towards Global Solutions

The strongest call for a global data localisation solution was the recent United Nations Conference on Trade and Development (UNCTAD) Digital Economy Report published on 29 September 2021. It

pointed out that the current state is that the greatest value is extracted from data by a small group of countries and large technology companies. Moreover, this is far below the optimal value that could be obtained. This is particularly disadvantageous for developing countries and their companies. The report points to the potential benefits of global regulation not only in terms of reducing inequalities between countries and increasing the added value extracted from data but also in increasing confidence in the digital economy. However, UNCTAD is currently not formally working on a global solution. There are also political and technical forums for global cooperation on international data flows, such as the e-commerce negotiations within the WTO. However, an agreement remains a long way off as developing countries, mainly China, indicate the need to explore the challenges and implications of data localisation before actual talks can begin.

However, an agreement remains a long way off as developing countries, mainly China, indicate the need to explore the challenges and implications of data localisation before actual talks can begin.

On the other hand, numerous attempts at regional and cross-regional solutions can be observed. Data is one of the main areas of work of the EU-U.S. Trade and Technology Council. The U.S., already within the framework of the U.S.-Mexico-Canada agreement replacing NAFTA or in the Trans-Pacific Partnership (TPP), has successfully pushed its liberal view on data flows, prohibiting their localisation by members of these agreements. Similar provisions are also found in bilateral trade agreements between many countries in the Asia-Pacific region.

A third route to the global standardisation of regulations is through certification schemes agreed at the inter-state level. They work in a similar way to the decisions issued by the EC on data transfers to third countries under the GDPR. They also represent a compromise between unrestricted data flows and numerous, incompatible national data localisation laws. The most popular such system is the CBPR created by APEC (Asia-Pacific Economic Community). Under the CBPR, organisations or countries that pass a verification process that confirms data privacy safeguards are free to process data from the territories of participating members. These currently include nine countries: Australia, Canada, Japan, Mexico, the Philippines, Singapore, South Korea, Taiwan, and the U.S.

Conclusions and Recommendations

In the coming years, globally, we should expect to see an increase in the number of data localisation laws, as well as an extension of their scope, for example to data in motion. Above all, this process will take place in authoritarian countries, led by Russia and China. These two countries are likely to block global attempts to regulate data flows at the WTO and UN levels. At the same time, certification schemes such as the CBPR will be developed and the number of regional agreements lifting existing restrictions will increase. This increases the risk of fragmentation (Balkanisation) of the internet, whose benefits are largely due to its existing open and decentralised architecture. Such fragmentation will not lead to the emergence of competing networks, but to the introduction of technical restrictions on some internet traffic. Countries that opt for such solutions, while gaining control over the digital sphere, will suffer negative economic consequences.

From the perspective of the European Union, the priority should be to reach an agreement with the main partner in the area of technology, the U.S., to build the greatest possible compatibility of the GDPR with other systems, especially the American one. To this end, it is particularly important to promote the EU model—which puts user data privacy at the centre—among developing countries, as well as to provide them with financial and technical assistance in this area. The further functioning of the open internet will depend on how broad a coalition of states the EU and the U.S. manage to build. This will have an indirect impact on the state of

The further functioning of the open internet will depend on how broad a coalition of states the EU and the U.S. manage to build.

democracy and the protection of human rights in the world. At the same time, the EU should intensify work on increasing the Union's data storage and processing capacity within the framework of ongoing projects. This will also reduce the costs of such services, lowering the barriers for businesses.