PACNET

JAPAN-KOREA LINE CONFLICT IS MORE ABOUT DATA SOVEREIGNTY

BY SEUNGHWAN (SHANE) KIM

SeungHwan (Shane) Kim (seunghwankim619@gmail.com) *is a Master's Graduate from the Johns Hopkins School of Advanced International Studies, focusing on security, statecraft, and East Asia. He is currently a researcher at the Korea Foundation. His previous experiences include roles at the East-West Center, the Maureen and Mike Mansfield Foundation, the Korea Economic Institute, and the Korea Studies Institute.*

Japan-Korea LINE conflict is more about data sovereignty

Data is considered a key component of artificial intelligence and information technology. With many superpowers and middle powers competing to become the vanguard of AI and IT services, data sovereignty is becoming increasingly significant worldwide. Data sovereignty refers to the idea that, just as national sovereignty resides with the people, the data generated by a country and its individuals should also be under their control. This means that countries and individuals or consumers should have the authority to decide when, where, how, and for what purpose their data is used.

With the ubiquitousness of the internet and AI, there is a growing emphasis on ensuring that the ownership of data can be determined by the nation and its people. Thus, nations have recently focused more on restricting and evaluating access to data—based on types of data and foreign entities—and strengthening data sovereignty.

Data sovereignty without differentiating partners and foes

On June 30, 2021, Didi Chuxing, often referred to as "the Chinese Uber," proceeded with its IPO on the New York Stock Exchange, raising $4.4 billion despite strong opposition from Chinese authorities. The officials had urged a delay, fearing the IPO documents might contain sensitive personal and geographic information about China. By July 2022, Chinese authorities imposed a fine of $1.19 billion on Didi Chuxing for violating cybersecurity laws, leading to the company's voluntary delisting. In response to these concerns, China enacted the Three Data Laws to regulate internet data processing, including the Cybersecurity Law, Data Security Law, and Personal Information Protection Law. These laws introduced measures like the Security Assessment Measures for Cross-Border Data Transfer, requiring government evaluations for transferring critical data overseas to protect data sovereignty.

In the West, including the US and Europe, China's actions against big tech and its data sovereignty measures have faced criticism for negatively impacting businesses. Yet, similar measures were soon adopted in these regions. For instance, the US Protecting Americans from Foreign Adversary Controlled Applications Act signed into law by US President Joe Biden last month, requires TikTok's parent company, Chinese firm ByteDance, to sell its US operations within 360 days or face a ban due to concerns that TikTok users' personal information could be accessed by the Chinese government. Prior to this, President Biden had signed an executive order in February to protect Americans' sensitive data, such as biometric, health, and location information, from adversarial nations like China. Additionally, countries such as Australia, the UK, and the European Union have banned TikTok on government devices and strongly recommend its removal from personal devices.

Europe has also been proactive in addressing data sovereignty. The European Union implemented the General Data Protection Regulation in May 2018, which regulates the transfer of data to third parties and nations unless explicitly permitted by the EU. It also grants individuals the right to control and delete their personal data. More recently, the Digital Markets Act and the Digital Services Act, which came into effect this year, aim to prevent market dominance by foreign big tech platforms like Google, Meta, and Apple, fundamentally seeking to protect domestic companies.

Missing Korea's data sovereignty

This trend of data privacy and restriction of where the data can go is prevalent in South Korea's neighboring

economies. The recent case of the Korea-Japan Naver Line conflict falls in line with this trend. The Japanese government pressured Naver to transfer its evenly divided shares to Japan's SoftBank due to fears that data from Line Yahoo, used by most Japanese, could be transferred to the Korean company Naver. This demand follows an information leak incident from Naver Cloud, which manages the Line messenging service most commonly used by Japanese consumers.

The issue began last November when Line Yahoo's servers were attacked, resulting in the leak of over 440,000 personal data records. Subsequently, on March 5 and April 16, the Japanese Ministry of Internal Affairs and Communications issued administrative guidance to Line Yahoo to protect the confidentiality of communications and ensure cybersecurity. This response highlights Japan's growing concern over data sovereignty and the use of Japanese data outside their jurisdiction.

Meanwhile, the Korean government focused solely on opposing the forced sale of Naver's shares, pledging to "firmly and strongly respond" to these measures. However, this reaction did not address the broader issue of data sovereignty protection. Compared to other major countries' policies to block foreign companies from collecting and accessing data, Korea's response appears overly complacent. The major reason is that Korean government continues to view data sovereignty protection merely as personal information protection. The current Personal Information Protection Act directly mentions in Article 1, Paragraph 1 that “the purpose of this law is to protect individuals' freedom and rights by stipulating matters related to the processing and protection of personal information and, furthermore, to realize the dignity and value of individuals.” It also briefly and vaguely stipulates in Article 14, Paragraph 2, the obligation of the state to formulate policies related to the transfer of personal information abroad and the obligation to obtain the consent of the information subject when transferring personal information abroad, not explicitly specifying its territorial scope. These limitations indicate that the Korean government continues to view data sovereignty protection narrowly, rather than viewing as a national security and a geopolitical issue. By not addressing the broader implications of data transfers and lacking a clear extraterritorial application, the PIPA falls short of the comprehensive measures needed to safeguard national data sovereignty in an increasingly interconnected digital world.

Recently, an Australian think tank reported that Chinese state-controlled propaganda agencies are extensively linked to collecting data from Chinese companies, including shopping and gaming apps like AliExpress and Temu. Despite these findings, relevant Korean ministries, such as the Ministry of Science and ICT and the Personal Information Protection Commission, have only mentioned observing how user data from Chinese online shopping companies is collected and used, which seems disconnected from the severity of the situation. While other countries implement policies to block foreign companies from collecting data and restricting where it can go, Korea still holds the outdated notion that as long as foreign companies manage collected personal information well and prevent cyberattacks following PIPA, it is not a big issue. This suggests that Korea may not fully understand the extent to which foreign companies operating in the country collect and use citizens' data. It is time for South Korea to adopt stronger measures to protect essential data for economic security and actively amend clear legislative standards that cover the extraterritorial scope.

PacNet commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed and encouraged.