ARI 124/2014
18 September 2024

Economic security vs economic coercion and data protection vs data protectionism: consequences and implications of the LINE Issue for Korea and middle powers

Yanghee Kim | Associate Professor, Division of Economics & Trade, College of Business, Daegu University

Theme

This paper examines the LINE issue to expose the emergence of new forms of protectionism in the age of artificial intelligence (AI) even among like-minded nations. In doing so, it clarifies the differences between economic security and economic coercion, as well as between data protection and data protectionism.

Summary

Major countries are trying to reinforce their economic security and data protection in the age of Artificial Intelligence (AI). As their national policies become more comprehensive in their conceptualisation and strict in their enforcement, there is a risk of unilateralism and instrumentalisation of these policies for protectionist purposes. The LINE issue encompasses contradictory features, economic security vs economic coercion, data protection vs data protectionism. Middle powers like Korea need to cooperate on economic security and data protection whereas opposing economic coercion and data protectionism when major states seek to develop sovereign AI.

Analysis

1. What is the LINE issue?

LINE is the most popular social media platform in Japan. It was created in Japan by Naver, a Korean web giant, in response to the country's severe destruction of communication facilities stemming from the earthquake in 2011. The platform has almost 200 million users worldwide, 96 million of whom are Japanese. Furthermore, LINE is a global platform including the LINE's platformer, Naver Cloud, the service developers of LINE such as Line Plus in Korea, as well as LY Corporation (LY), Line Corporation (Line), other service developers such as Demaekan, and LINE users in Japan and abroad.

In March 2021 Naver sold a half stake to SoftBank (SB), a Japanese IT giant to establish A Holdings, which owns 63.6% of LY that has a wholly owned subsidiary, Line Corporation (Line) managing the LINE platform. Naver and SB agreed that the former is responsible for technical development and maintenance, while the latter oversee all aspects of LINE's operations in Japan and abroad. So, Naver has little involvement in LINE's management.

The first LINE scandal occurred in March 2021. There were multiple unauthorised accesses to Line's affiliate in China. Fortunately, neither unlawful activities nor confidential information leak were founded. As a result, Japan's Personal Information Protection Commission (PPC) and the Ministry of Internal Affairs and Communications (MIC) released administrative guidance known as 'advice', based on the Act on the Protection of Personal Information. According to the Act, when a personal information leakage incident occurs, the PPC can require the following measures to be taken: report submission, on-site inspection, guidance, advice, recommendations, and orders, according to the gravity of the incident. Among them are recommendations and orders, which are measures towards a violation of the act. The event at the Chinese affiliate had a significant influence in Line. Following the enactment of the National Intelligence Act by the Chinese government in 2018, which could allow the authority to monitor personal data, including that of foreign companies, Tokyo regarded the Line incident in China as a significant risk to Japan's national security, despite the fact that the data were stored in Japan and Korea. This security failure instilled a great suspicion at Naver in Japan, particularly among right-wingers of the Liberal Democratic Party (LDP). Nonetheless, the multi-factor authentication mechanism that Naver and LY had promised the Japanese government in 2021 that they would create did not go live until 2023.

In August 2023, the 'LINE issue' occurred. Initially, a computer belonging to an employee of a subcontractor used by Naver Cloud was infected with malware in Korea. Given that Naver Cloud and LY shared an authentication system, this resulted in infection of LY's internal server, leading to the disclosure of around 520,000 pieces of personal information. However, there has been no indication that the information has been used for criminal purposes.

The Japanese authorities outlined that the incident was caused by LINE's excessive technological reliance on Naver and inadequate governance of information protection at LY and Naver. Thus, Line was given a 'recommendation'. It is worth mentioning, however, that the MIC and PPC's policy directions differed on the steps to be taken by the LY. The MIC suggested enhancing security measures in both technological and organisational aspects, such as revising Naver's share ratios. This assumes that LY may face challenges in demanding robust security measures from its parent firm, Naver. Conversely, the PPC's recommendation to LY, which was issued twice, did not contain the requirement. If it will enhance privacy according to PPC criteria, the agency should have explicitly mentioned this. LY's report to the MIC stated that it had initiated discussions with Naver to alter its ownership, whereas its report to the PPC did not acknowledge this.

The matter appears to have been resolved, after the positive response from the MIC to LY's second report on 1 July. The ministry urged that it had not requested Naver's stake sales. As early as 8 May, though, SB had disclosed that it was in talks with Naver to buy further shares. Finally, LY's second report acknowledged the improbable completion of the stake adjustment deal. Consequently, the issue has been put on hold.

2. Economic security vs economic coercion

Nevertheless, the term 'economic security' has become a buzzword in recent years, appearing in a variety of contexts, with only a few states providing a precise definition in their policies. For instance, Japan declares that 'economic security is to ensure Japan's national interests, such as peace, security, and economic prosperity, by carrying out economic measures'. Korea defines it as 'a state in which economic activities are unimpeded and national security is preserved by ensuring the smooth inflow of essential items for the nation's economic activities and preventing inappropriate outflow, regardless of domestic and international variables'.

Industrial policies, investment screening, export controls, economic sanctions, cybersecurity and data protection, addressing economic coercion, and assuring the resilience of critical infrastructure and supply chains are all part of economic security policy. Some of these policies are reactive, responding to threats or risks, while investment screening, export controls or economic sanctions are proactive measures. Alternatively, some proactive measures could be perceived as economic coercion.

Economic coercion can be defined as 'a threatened or actual imposition of economic costs on one state by another with the objective of extracting a policy concession'. The Countering Economic Coercion Act of 2023 was enacted by the US Congress on 3 July 2023. It defines economic coercion as 'the intentional use of actions, practices, or threats by a foreign adversary to unreasonably restrain, obstruct, or manipulate trade, foreign aid, investment, or commerce in order to achieve strategic political objectives or influence sovereign political actions'. China is notorious for employing economic coercion in a variety of forms. In contrast to Western sanctions, which are subject to court challenges and adhere to formal legal procedures, Chinese measures are frequently informal.

It is challenging to differentiate between economic security and economic statecraft or economic coercion. The term 'coercive economic statecraft' has been employed by a reputable think tank as a valuable toolkit for the US. The state has initiated implementation of its measures, including tariffs, export controls, supply chain restrictions, inbound investment reviews and import restrictions, such as the prohibition of Chinese applications like TikTok, in order to achieve a diverse range of objectives, according to the report.

Even countries that share similar values often implement such coercive measures. For example, the Trump Administration implemented tariffs on steel and aluminium imports from allies, on the grounds that the volume of imports posed a threat to US national security. Another notable example is Korea. It is important to note that Korea was subjected to economic coercion by both China and Japan. Some, such as Farell & Newman (2019), perceived Japan's 2019 tightening of the export prohibition on Korea as a weaponisation of interdependence or economic coercion. It was an open secret that the objective was to restrict the Korean Supreme Court's implementation of the ruling that Japanese companies are obliged to compensate for the forced labour of Koreans taken to Japan during its colonial rule.

This shows that the distinction between economic security and economic coercion is subjective, subtle and ambiguous in practice, irrespective of whether it is formal or informal, explicit or implicit, or directed at adversaries or allies.

3. Data protection vs data protectionism

According to the 2017 data policy restrictiveness Index by Janez Kresn *et al.* (2018), which analyses 64 major economies, Russia, China and Turkey are the highest, followed by France, Germany and Korea, while Japan ranks 46th. Japan was the first country to advocate the concept of 'data free flow with trust' in 2019. Japan has included the so-called 'TPP three principles', which are high-level digital trade regulations, in the US-Japan Digital Trade Agreement, Japan-UK EPA and CPTPP, including free cross-border data transfer, no data localisation and no forced disclosure of source codes and algorithms. The EU-Japan deal on cross-border data flows entered into force on 1 July 2024 and is likely to be included in the EU-Japan EPA. It allowed no data localisation requirement.

However, there is an increasing movement towards 'data protectionism', which centres on the regulation of 'data localisation'. Data localisation refers to the more explicit requirement that data be stored and/or processed within the national territory (López González, J., *et al.*, 2022). By 2021 there were 92 regulations in 39 countries, more than half of which had emerged in the previous five years. López González *et al.* (2022) identify the following policy objectives as reasons for data protectionism: privacy, national security, data security, intellectual property protection, digital protectionism, data sovereignty, competition policy, industrial policy and taxation policy.

Opponents of data protectionism argue that it has a detrimental economic impact. From a national security standpoint, demands to retain servers in-country can be problematic owing to earthquakes, unpredictable power circumstances, political crises and so on. In response to a potential Russian invasion in 2022, Ukraine modified its statute requiring onshore storage and transferred some government and private enterprise data to Amazon Web Services in the US. Japan's NTT and SB established a data centre in Korea to back up data following the 2011 Great East Japan Earthquake. Therefore, it is unclear whether localising servers and totally reshoring LINE will contribute to economic security in Japan.

The right to privacy, development issues related to data sovereignty, and potential public issues suggest the need for data protection (Ferracane, M.F., *et al.*, 2018). The EU emphasises 'data protection, no to data protectionism' and insists on trade agreements in line with the European General Data Protection Regulation in 2018. More recently, economic security has also emerged as an important rationale for data protection, blending many of the above policy objectives. In particular, the US House of Representatives' TikTok Ban Act is a case in point. The US used similar vetoing rationales to the WTO's plurilateral Electric Commerce deal, which almost reached a draft, and took a defensive stance in the trade pillar of the Indo-Pacific Economic Framework (IPEF) deal. The Biden Administration apparently believes that data free flow could unduly favour the interests and influence of platform giants. The EU is leading a

data protection wave related with privacy and civil rights. It has pioneered the deployment of the EU AI Act, a comprehensive regulation on AI related risks.

Data protectionism, however, overlaps with data protection to some extent. If the criteria are arbitrary or non-transparent, as in the Countering Economic Coercion Act of 2023, Japan's recent actions could move further from economic security and data protection to economic coercion and data protectionism. Although Japan opposes data protection in terms of policy, its competitive edge in related fields such as cloud, platform and AI is less competitive as the government is concerned about reliance on foreign companies. It shed light on data protectionism, which covers the desire to encourage platform and AI localisation. As with the TikTok ban in the US, the distinction between data protection and data protectionism is ambiguous and very contentious.

4. Japan's responses to the LINE issue

In April 2021, following the incident with the Chinese Line affiliate, the Japanese government issued a guideline prohibiting government agencies and local governments from handling confidential information via LINE. In May 2022 Japan introduced the Economic Security Act. It focuses on ensuring the stable provision of specified essential infrastructure services, among other things. In November 2023, 210 service providers, including LY, were designated as 'specified essential infrastructure services providers'. Japan also designated cloud services as 'specified critical facilities' under the Act. On 10 May, the House of Councillors of Japan passed the Law on the Protection and Utilisation of Important Economic Security Information. The law requires those who handle important economic security information to be certified by the government.

It is important to understand that Japan's responses to the LINE issue differ from agency to agency since they have varying implications for Korea and other middle powers' future response and challenges. The PPC appears to take a privacy-focused approach, yet the MIC monitors specific infrastructure operators under the Economic Security Act. Furthermore, the Liberal Democratic Party, Japan's long-ruling party, is largely concerned with economic security and data protection, connected with industrial policy for promoting sovereign AI.

Ironically, the MIC's extraordinary demand for a stake sale at Naver veiled the company's information management deficiencies in Korea, and Japan's response was perceived as economic coercion. This fuelled a Korean backlash. The number of newspaper articles regarding 'LY' reached a high, to 206, on 13 May, from one or two per day by mid-April in Korea. The Korean government was initially reluctant to intervene directly, stating that the MIC's demand did not mean Naver's divestment. Nevertheless, a significant number of Koreans, who have not forgotten Japan's previous imposition of an export restriction on Korea as a kind of economic coercion, are experiencing a growing sense of animosity towards Japan. Opposition parties perceive this issue as Japan's deliberate endeavour to obtain control over LINE. The environment was characterised by a growing anti-Japan sentiment. On 13 May Naver's labour union expressed its opposition to the compulsory Naver stake sale. Under these circumstances, on 14 May, the Korean presidential Office announced that the report due to the MIC on 1 July will not contain the sale of the Naver

share. It further argued that the Japanese government ought not to penalise Naver for this.

It would be helpful to understand why the MIC demanded Naver's divestment from Japan. Some within the LDP have advocated LINE's 'Japanisation', as well as a reduction in Naver's shareholding ratio, to limit its control over LINE. Furthermore, some suggested that the Foreign Ministry, Ministry of Defence and Self-Defence Forces refrain from using LINE, and that local governments do not create new LINE accounts until LY's recurrence prevention measures have been fully implemented.

Nevertheless, the LDP's direct role was revealed by *Mainichi Shimbun*, a major Japanese newspaper. Between March and April, Akira Amari, the chairperson of the Headquarters for the Promotion of Economic Security Council of the LDP, met the founder and chairman of SB Group, Masayoshi Son. Amari asked Son to ensure that Japanese infrastructure (LINE), from app development to everything else, would be complete in Japan. Amari is an influential politician who was the Party's former Secretary General and has held ministerial positions in multiple ministries. He is a well-known member of the *Nippon Kaigi*, an ultranationalist far-right organisation. Given his presence in Japan, it is hard to assume his meeting with Son was personal. A senior ministry official of the MIC also met SB's CEO, Junichi Miyakawa, while the MIC requested a stake sale in Naver. SB officials were astonished by the extent of government intervention. The Mainichi Shimbun also claimed on 1 July that the ministry's unusual reaction was 'an attempt to correct the control of Naver'. It reveals that a major far-right lawmaker in charge of economic security actively advocated for the MIC demand. It is also unusual for a politician to meet the joint venture's local counterpart in today's market economy. Although SB is unlikely to purchase additional stakes from Naver in the near future, it is obliged to end its business relationship with the company. As stated by the *Mainichi Shimbun*, the LDP's activities also have an industrial policy component, as it intends to promote the local AI-related ecosystem. Korea viewed the decision to force Naver's divestment as a combination of economic coercion and anti-Korean animosity.

In an annex to its second report to the MIC, LY highlighted its plans to disentangle not only the technological stacks but also the entire relationship with Naver by the end of 2025. LY's alternatives to Naver are technology internalisation and a shift to a third party in Japan. This was in response to the MIC's specific request for information on when and how LY's tie with Naver should be terminated. It was exactly what Amari advocated. The annex, combined with the unseen enforcing power of administrative guidance, which is not legally binding, can be interpreted as economic coercion against a JV in the name of economic security.

5. Consequences for Naver and SoftBank

The primary concern for Naver is the negative impact on its management. To begin with, the termination of ties with SB will have an impact on its global business operations, which are heavily dependent on LY as a gateway to overseas businesses. By 2023, Naver had developed 106 overseas affiliates. Of these, around 26% are Japan-based subsidiaries, while the largest shareholders of subsidiaries in foreign countries under LY's control account for around 73% of the total. Under these circumstances, around

2,500 employees of LY's subsidiaries in Korea, who oversee LINE's global operations, are opposed to Naver's forced stake sale. They were concerned that this might result in job insecurity and technology exposure from LY's Korean affiliates to Yahoo owing to a lack of a comparable technological cumulation in Yahoo, and challenges for global business.

Furthermore, Naver's global business disruption may limit its access to data for AI collected in Japan and South-East Asia through LINE. On 25 November 2020, before LY formally launched, Line announced that it would develop the world's first large-scale language model (LLM) for Japanese in collaboration with Naver. At an earnings conference on 10 May 2023, SB's CEO Miyakawa announced that it was working with Line to launch a Japanese GPT based on HyperCLOVA, a LLM developed by Naver and Line. 'We are the only company in Japan that has the basic base for GPT. CLOVA has a vast amount of domestic data, and we aim to provide excellent services for the domestic market', the CEO said. However, in 2024 SB is creating an LLM with others but without Naver.

What are the main reasons SB changed its partner, Naver, with whom it had collaborated for nearly four years to build sovereign AI? One SB insider I spoke to believes it is due to HyperClOVA's weaker performance compared with others. However, it is reasonable to interpret that the LINE incident was also a trigger and justification for LDP to request SB's split with the distrusted Naver for the sovereign AI. 'Son, the founder of SB group envisioned creating a global tech platform via LY but his vision will naturally clash with what the Japanese government is trying to do from an economic security perspective', said a professor and economic security expert at the University of Tokyo. The Japanese Ministry of Economy, Trade and Industry has awarded SB with up to ¥47.4 billion in developing supercomputers and clouds in accordance with the Economic Security Act since 2023.

Naver did not welcome the Korean public's intense attention and the Korean government's involvement in the LINE issue, despite the MIC's unexceptional action, for the following reasons. First, Naver was going to sell its partial share of A Holdings for business considerations. However, since the LINE episode galvanised the Korean public against the MIC's forced sale, Naver had to hold on to it for a while. Secondly, as Naver responded to the Korean authorities in July, it felt that LY, not Naver, is liable for LINE's cyber security risks, based on its capital structure and the agreement between Naver and SB. This contradicts the logic of the MIC. Third, over the past 13 years, Naver was obliged to show LINE as 'made in Japan' by establishing a JV with SB to thrive in the nationalistic market. So Naver did not want the Japanese to perceive LINE as 'made in Korea'. It is critical to understand the Japanese market, in which right-wing anti-Korean prejudice exists. Platforms headquartered in the US never need to worry about this.

It is difficult to say if the LINE issue is favourable to SB. The latter is claiming that buying more Naver shares is unnecessary because it already controls LINE. The annex to LY's 1 July report to the MIC underscores the problems it faces in reducing its technological reliance on Naver soon. For example, LY's proposed date of December 2025 for decoupling from Naver is simply a target, with a short footnote indicating that it could be

extended depending on the risk assessment. The importing of joint results with and offerings from Naver took place as an alternative to cutting the business contractions with Naver as well. There are no criteria, however, for third parties in Japan. The MIC's unusual demand for Naver's divestment resembles Japan's strengthened export bans, *de facto* economic coercion or weaponised interdependence from the Korean perspective.

Conclusions

To sum up, there are a number of important questions raised by the MIC's demand that Naver divest. First, does LY's information security not increase with Naver and LY's technological separation? Not really. It does not matter because SB already owns LINE and is in charge of upholding security governance. Secondly, does the MIC's demand align with the global 'proportionality' principle? Not really. LY's flaws are obviously unacceptable, but it is unjustifiably severe compared with LINE's issue with both Naver and SB. Japan should hold off on pushing for a change in the shareholding structure until after it has had a chance to evaluate the efficacy of LY's information security procedures. Is it feasible to claim that this is not economic coercion while at the same time justifying everything in the name of economic security? Not really. It is true that there is less of a line between economic coercion and economic security.

The LINE issue triggered a fresh wave of protectionism in Korea. The incident demonstrates that Japan's economic security can be viewed as economic coercion: not the information breach itself, but Japan's unexpected reaction that followed. The LINE incident highlights that Japan's data protectionism can be rationalised as data protection. The episode revealed that like-minded nations can use economic coercion or data protection at any time. Nonetheless, the distinctions between economic security and economic coercion, as well as data protection and data protectionism, have important practical implications. Improving economic security is especially important for Korea and other middle-power states in the era of superpower strategic confrontations. The trend of a few states building sovereign AI based on their own history, culture and language emphasises the importance of data sovereignty for Korea and other middle powers. They should promote economic security and data protection while opposing the economic coercion and data protectionism employed primarily by superpowers.

This contrast underscores the importance of cooperation, notwithstanding the tensions between Korea and Japan over the LINE platform. They are both involved in a variety of international cooperation schemes, like the CPEA, aimed at protecting personal data. However, there has been little evidence of collaboration or coordination between the two after the LINE incident. Instead, they should both make use of the chance to widen their views and embrace data protection coordination in order to prevent similar incidents from occurring again.

Apart from the benefits that protectionism brings to local enterprises, there is an urgent need for international cooperation on economic security and data protection in the new AI era for the benefit of Korean and Japanese citizens as well as the public interest.