This abstract was submitted to and presented at CCRC International Conference 2022.

Digital Trade and National Security: A Search for a Better Balance

Rikako Watai, Professor of Administrative Law, Keio University Law School, Japan

INTRODUCTION

The spread of the internet has transformed economic transactions, and digital markets have expanded across the globe. Over the past two years, the ongoing COVID-19 pandemic has also accelerated the development of digital trade[1]. Since its establishment in 1995 as a new organization that would develop to replace the 1947 General Agreement on Tariffs and Trade (GATT), the World Trade Organization (WTO) has set comprehensive international trade rules for goods and services. But rules are not yet in place for digital trade, and in January 2019 a number of countries came together on a voluntary basis to release the Joint Statement on Electronic Commerce[2], prompting discussions that continue to this day.

The rules of individual countries on digital trade do not necessarily coincide. The United States is home to IT platformers like Google, Apple, Facebook, and Amazon.com (GAFA) [3], which means that private-sector companies exert a powerful influence on the rule-making process. By contrast, the European Union formulated the General Data Protection Regulation (GDPR) in 2016 and has followed a policy based on protecting personal information, taking an approach to rule-making that focuses on individuals rather than businesses. In China, the government takes the lead on data management, through a legal system that limits cross-border transfer of data and requires that data be stored within China's borders[4].

Japan has also developed its own approach. At the World Economic Forum annual meeting in

[1] Although no globally agreed definition yet exists for digital trade, the Organisation for Economic Co-operation and Development (OECD)'s definition, "digitally-enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve consumers, firms, and governments" has become quite established.
[2] World Trade Organization, Joint Statement on Electric Commerce WT/L/1056, 25 January 2019 (19-0423).
[3] In October 2021, Facebook announced that it would change its company name to Meta.
[4] Yoshinori Abe, *Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures?*, 16 Public Policy Review 5, 1, 3-4 (Policy Research Institute, Ministry of Finance, Japan, Feb. 2021). https://www.mof.go.jp/english/pri/publication/pp_review/ppr16_05_02.pdf (last visited Jan. 10, 2022).

January 2019, then Prime Minister Shinzo Abe announced Japan's concept of Data Free Flow with Trust (DFFT), and this was included in the Leaders' Declaration at the G20 Osaka Summit in June. DFFT outlines the position of the Japanese government, which aims to achieve a balance in drawing up digital trade rules between data security and user confidence on the one hand and the free and open flow of data on the other. Since coming to office in November, the new cabinet under Prime Minister Fumio Kishida has announced that economic security will be its biggest priority[5]. The relationship between economic security and digital trade is not yet clear, but data is clearly of major importance in a digitalized society, and data leaks have the potential to cause national security problems. It is necessary to consider the balance that needs to be struck between promoting digital trade and national security concerns.

THE DEVELOPMENT OF DFFT

DFFT is an approach based on the idea that guaranteeing privacy, security, and the safety of intellectual property as the foundations of data flow will help to encourage the free flow of data. Central to the approach is the idea that data flow should be "with trust." The US-Japan Digital Trade Agreement signed in January 2020 aims to construct a new trading area through the free flow of data, and DFFT is an attempt to embody this and put it into practice. The treaty includes relevant provisions on: a ban on imposition of customs duties (Article 7), non-discriminatory treatment of digital products (Article 8), freedom of cross-border transfer of information (Article 11), a ban on requirements for data localization (Article 12), a ban on requirements for disclosure of source code (Article 17), and a ban on demands for access to cryptography (Article 21). Of these, the prohibitions of demands for data localization, disclosure of source code, and access to information using cryptography can be said to involve the "with trust" concept.

Data localization requires a business to locate facilities and related data within a country's borders as a condition of carrying business there. Regulations based on this requirement might include bans on transfer of data, or requirements affecting the retention and storage of data acquired and collected for the purpose of corporate activities. If data transfer is restricted by strict data localization requirements, this will inhibit the free flow of data. Also, if compulsory access by public institutions to information held by private-sector companies (government access) is used to secure an advantage for that country's industries, such moves would surely not only violate WTO agreements, but also go against the promotion of digital trade. Some government access, however, such as in criminal investigations, can be regarded

[5] Brad Glosserman, *Kishida doubles down in economic security*, Japan Times (Oct. 12, 2021) https://www.japantimes.co.jp/opinion/2021/10/12/commentary/japan-commentary/kishida-economic-security/ (last visited Jan. 10, 2022).

as legitimate, provided proper legally defined procedures are followed. The question is what other circumstances should be regarded as legitimate reasons for limiting the free flow of data. Most people would probably agree that national security should be included as a legitimate reason. For example, taking steps to prevent the leak of important technology essential to national security would probably be regarded as legitimate, and provisions to allow this would not violate WTO agreements, so long as the necessary minimum measures were taken.

Although no clear definition of "national security" exists[6], as far back as GATT, Article 21 contained provisions on Security Exceptions that allowed countries to take steps to limit free trade based on national security considerations. Article 4 of the US-Japan Digital Trade Agreement also contains national security exceptions. Consequently, even in agreements based on the principle of free trade, the necessity of exceptions from the perspective of national security concerns has been recognized for more than 50 years.

Article 21(b) of GATT states that "nothing in this Agreement shall be construed … to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests: (i) relating to fissionable materials or the materials from which they are derived; (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment; or (iii) taken in time of war or other emergency in international relations." These provisions recognize that a state has a legitimate right to protect its essential security interests, but it is fair to say that the reasons envisaged for these exceptions refer to an extremely limited set of circumstances.

The security exceptions in Article 4 of the US-Japan Digital Trade Agreement stipulate that "nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests." This suggests that the grounds for application of these exceptions may be somewhat broader than those in GATT Article 21[7]. If these exceptions were applied frequently, they would probably have the potential to damage the intent of the agreement.

---

[6] Rikako Watai, *Digital Trade and National Security Exceptions*, 27 Int'l Trade L. & Reg. 2, 119, 123 (2021).

[7] Similar provisions are included in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).

NATIONAL SECURITY AND DIGITAL TRADE

The Kishida administration has established a new ministerial post for economic security, and preparations are underway for draft legislation on the promotion of economic security to be submitted during the ordinary session of the Diet in 2022. Four topics have been set as priority areas to be addressed in the draft legislation: a more robust supply chain, ensuring the security and reliability of key infrastructure, technological cooperation between the government and private sector, and non-disclosure of patents in sensitive areas[8]. Since economic security means taking necessary steps to guarantee the economic autonomy of the country for strategic reasons, it is likely that this will have a certain impact on digital trade.

As with the concept of national security itself, no fixed definitions exist for economic security. In Japan, discussions began from the definition agreed by the Industrial Structure Council's Special Sub-Committee for Economic Security Issues in 1982: "Economic security means defending the country's economy from major threats arising internationally, chiefly by employing economic means." [9] In June 2021, the Japanese government's Basic Policy on Economic and Fiscal Management and Reform 2021[10] outlined the strategic direction for economic security as follows: "The Government will expand and deepen cooperation with like-minded countries under the international order based on fundamental values and rules, and will seek to ensure Japan's self-determination and acquire advantages for our country," noting that "from this perspective, the Government will implement concrete measures and policies to strengthen its efforts to identify, protect, and develop critical technologies and to enhance the resilience of essential industries." It seems that economic security is understood as representing the basis foundations for free trade.

DIGITAL TRADE AND NATIONAL SECURITY EXCEPTIONS

At the G7 Digital and Technology Ministers' Meeting in July 2021, agreement was reached on a roadmap for cooperation on DFFT, and since the 2023 G7 summit is due to take place in Japan, moves to secure the status of DFFT as an international system are likely to gather pace

---

[8] Isabel Reynolds and Emi Nobuhiro, J*apan Economic Security Minister Says Business Must Be Free,* Bloomberg (Nov. 26, 2021) https://www.bloomberg.com/news/articles/2021-11-26/japan-economic-security-minister-says-business-must-be-free (last visited Jan. 10, 2022).
[9] Special Sub-Committee for Economic Security Issues (*Keizai anzen hosho mondai tokubetsu shoiinkai*), Industrial Structure Council, "Keizai anzen hosho no kakuritsu o mezashite" (Toward the establishment of economic security), (April 28, 1982) 27.
[10] Cabinet decision: "Basic Policy on Economic and Fiscal Management and Reform 2021 (English version) Four Driving Forces that Open the Way to the Future of Japan: Green, Digital, Creation of Vibrant Local Regions, Measures against Declining Birthrate" (June 18, 2021) 28.

in the years to come[11]. In drafting rules for digital trade, the positions of each country differ, but efforts to bridge these gaps are likely to continue. It is not uncommon in drawing up rules among states to reserve policy space for national security issues, and such provisions are also necessary from the perspective of ensuring that the rules operate "with trust." Ambiguity remains, however, particularly with regard to where to draw the line between "national security" and "protectionism." There is a need for thorough-going discussions of plausible situations in which national security might become an issue in digital trade. States have broad political and policy discretion in invoking the security exceptions, and how to control this is likely to be a challenge.

It is to be hoped that in the future, the approach to the free use and application of data put forward in the US-Japan Digital Trade Agreement will continue to find wider acceptance and will eventually develop to be adopted as part of WTO rules.

[11] The roadmap included four main points: an assessment of evidence on the impact of data localization, a comparative analysis of each country's policies on cross-border data transfers, formulation of guidelines for trusted government access, and steps to accelerate the development of mutually acceptable sharing of data.