

Data Law Aspects of Commercial Satellite Remote Sensing: New Challenges for the New Opportunities

*Souichirou Kozuka and Mayu Terada**

Abstract

As the commercial satellite remote sensing has grown to bear the typical features of data industry, the relevance of data law to this industry sector has become apparent. However, the data law differs significantly from one jurisdiction to another. The difference is especially big with regard to the regulation on profiling. Given such feature of data law, it should be crucial that the data law does not undermine the internationally recognised principle of the freedom of remote sensing activities, pronounced in the United Nations Principles of Satellite Remote Sensing. It is the cause of difficulties that the commercial satellite remote sensing faces, because the satellite data most likely threatens the personal privacy when used as part of the “big data” and identifies a person through profiling. One possible solution may be to interpret and implement the data law in a manner that least compromises the principles on satellite remote sensing developed by the space law. Another, more practical solution is to develop private arrangements, requiring the data provider to guarantee compliance with the relevant data law, as well as indicating the standardised conditions for trade in data on the platform. Lawyers should find the way to respect both the space law and data law and ensure that the “free flow of data with trust” is realised for satellite data.

Keywords: commercial satellite remote sensing, satellite data, personal data law, platform

* Souichirou Kozuka, Faculty of law, Gakushuin University. Mayu Terada, Department of Politics and International Studies, International Christian University.

1. Introduction

1.1. The Aim of This Paper

In this paper, we are going to argue that the satellite remote sensing raises not only the space law issues, but data law issues as well.

The legal discipline over the satellite remote sensing has been discussed by space lawyers for decades. Besides the international law framework over the activities, several states have introduced domestic regulation over the satellite remote sensing activities by non-governmental entities. These states include the United States, Canada, Germany, France and Japan.¹ In a state where no such specific regulation is enacted, non-governmental remote sensing activities may still be regulated by the general law on space activities.²

These laws controlling the permissibility of the remote sensing activities have been well examined. In contrast, legal issues arising from the products of such activities have largely been neglected. Some documents on the commercial satellite remote sensing mention the issue of privacy as a possible source of concern when facilitating such activities, but in-depth analysis of the issue has not been made.³ We believe that the application of the data law to products from satellite remote sensing activities is an issue needing a solution in practice when the market for satellite data is developing rapidly.

1.2. The Backgrounds of the Problem

To start with, we need to recognise that the recent commercialisation has brought about big changes to the satellite remote sensing activities. While the commercialisation has been observed since 1980s, when the United States attempted to privatise its Landsat system and France considered ensuring source of revenues for SPOTImage,⁴ the recent developments in technology have transformed the industry extensively. It has become possible to achieve high resolution by much smaller satellites than before. This has enabled the

1 F. Tronchetti, Legal aspects of satellite remote sensing, in: F. von der Dunk & F. Tronchetti (eds.), *Handbook of Space Law* (Edward Elgar, Cheltenham and Northampton, 2015), 501-553.

2 A. Ito, *Legal Aspects of Satellite Remote Sensing* (Nijhoff, Leiden and Boston, 2011).

3 Digital Transformation Monitor, *Big Data in Earth Observation* (July 2017), https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Big%20Data%20in%20Earth%20Observation%20v1.pdf, (accessed 15.1.2021); I. Baumann & E. Pellander, 'New Legal Issues in Earth Observation Data and Services', in: M. Hoffmann & P.J. Blount (eds), *Innovation in Outer Space: International and African Legal Perspectives* (Nomos, Baden-Baden, 2018), 171-186; M. Sudmanns et al., 'Big Earth data: disruptive changes in Earthobservation data management and analysis?', [2020] 13(7) *International Journal of Digital Earth* 832-850.

4 Tronchetti (fn 1); Joanne Irene Gabrynowicz, 'The Perils of Landsat from Grassroots to Globalization: A Comprehensive View of US Remote Sensing Law with a Few Thoughts for the Future', [2005] 6(1) *Chicago Journal of International Law* 45-67.

commercial operators to deploy small satellites to constitute a constellation and realise more frequent visits to the same spot.

As a result, the one-off “sale” of a piece of imagery (which is, legally speaking, the license of rights to the imagery) is no longer a standard format of transaction in this industry sector. Data is supplied as a continuous stream and is often processed automatically without the human intervention, using the machine learning technology.

Furthermore, it has become usual to trade data over a platform. The platform for satellite remote sensing data, as with any other platform in the digital economy, is a two-sided market. It attracts data providers on one side and data users to develop secondary products on the other side. Some platforms are maintained by the commercial entity, while some others have been created by the government aspiring to build the national platform.⁵

These developments mean that the commercial satellite remote sensing bears the typical features of the data industry. This is the background that the data law, besides the framework of space law, has become relevant to the commercial satellite remote sensing.

1.3. The Structure of This Paper

The remaining sections of this paper proceed as follows. First, we explain how the data law causes difficulties to the satellite remote sensing, focusing on the apparent inconsistencies of the space law and data law on the subject of satellite remote sensing (2). Then we examine the personal data laws of major jurisdictions in depth and point to their divergences (3). Based on these examinations, we advance the practical solutions, for both the short and the longer term (4). In the final section we conclude by emphasising that the lawyers in space law and data law need to make dialogues with the experts in the industry (5).

2. The Apparent Inconsistencies of the Space Law and Data Law Concerning the Remote Sensing Activities

2.1. The Resolution of Satellite Data and Privacy

Although the capabilities of commercial remote sensing satellites are improving, the resolution is not high enough to identify a person yet. Therefore, it might sound curious to consider the data law, in particular personal data law, to be relevant. However, the data collected from satellites can be used with the data from other sources, constituting the pool of data as “big data”.

5 C. Jabbour et al., ‘Spatial data infrastructure management: A two-sided market approach for strategic reflections’, [2019] 45 *International Journal of Information Management* 69-82.

When the data from the satellite becomes part of the “big data”, profiling of a person may become possible through the integrated analysis of the data. For example, even if a piece of imagery from the satellite does not identify a specific person, information from other sources, such as the location of the building in the residents registry, types of cars coming in and going out of the place captured by a nearby surveillance camera and the consumption data of electricity collected through a home sensor, may enable an observer to name the person in the satellite imagery.

2.2. The Basic Principles of the Outer Space Law on Remote Sensing

It is important to recall that the fundamental principle of the space law on satellite remote sensing is the freedom of activities. The Outer Space Treaty pronounces in its very first Article that the outer space “shall be free for exploration and use by all States”. The Principles Relating to Remote Sensing of the Earth from Outer Space (hereinafter “PRS”), adopted by the United Nations Assembly as Resolution 41/65 in 1986, refer to this Article of the Outer Space Treaty in the Principle IV and confirm the freedom of remote sensing from the outer space.⁶

It is true that this principle of the freedom of satellite remote sensing does not stand alone but is accompanied by the right of the sensed State to have access to the data under certain conditions as pronounced in the Principle XII.⁷ However, the right of access of the sensed State does not limit the remote sensing activities. Rather, it underscores the will of the international society to facilitate the use of the data from satellites. Thus, it may be said that the space law firmly establishes and advocates the freedom in collection and use of satellite data.

The internationally recognised freedom of satellite remote sensing has further been developed under the global cooperation scheme of GEOSS (Global Earth Observation System of Systems).⁸ Launched in 2005, the GEOSS has advanced the open exchange of data. In 2015, the rule developed into the “full and open” exchange of data. These rules on the exchange of data under the GEOSS framework does not apply to data from commercial satellite. Still, the principle of freedom in satellite remote sensing is also important for commercial operators. It is because such freedom of satellite remote sensing is

6 Tronchetti (fn 1); S. Mosteshar, ‘Regulation of remote sensing satellites’, in: R.S. Jakhu & P.S. Dempsey (eds), *Routledge Handbook of Space Law* (Routledge, London and New York, 2017), pp.144-159.

7 L.J. Smith, ‘Principle XII (data Access on Non-Discriminatory Basis)’, in: S. Hobe, B. Schmidt-Tedd & K.-U. Schrogl (eds), *Cologne Commentary on Space Law*, Volume III (Carl Heymanns Verlag, Köln, 2015), pp.162-169.

8 S. Aoki, ‘The Function of ‘Soft Law’ in the Development of International Space Law’, in: I. Marboe (ed), *Soft Law in Outer Space: The Function of Non-binding Norms in International Space Law* (Böhlau Verlag, Wien, Köln, Graz, 2012), pp.57-85.

the advantage vis-à-vis the remote sensing from airplanes or drones, which are subject to the rules and regulations of the territory.

2.3. The Issues Raised by the Data Law

While duly noting the relevance of data law, it is important to ensure that the data law does not compromise the principle of freedom established by the space law. The role of data law should be to add trust to the use of (personal) data, which will ultimately facilitate the use of such data. This holds for data from any source, but must be taken particularly seriously for the data from satellites, for which the principle of freedom has been established and internationally recognised.

However, the problem arises from the fact that the space law applies globally, while the personal data law is domestic and lacks global harmonisation. Even the basic policy varies across jurisdictions, still more the scope of, and approaches to, the regulation. It is especially true with regard to the issue of profiling, mentioned above. The fragmented status of the personal data law poses a challenge to data users, who have to comply with every applicable personal data law on each piece or set of data. If the user faces difficulties, the data providers are also discouraged, due to the nature of the platform as a two-sided market.

3. Different Regulation on Data and Privacy

Data law and its regulation are quite differently written and implemented from countries to countries.⁹ It is pointed out that the notion of data controller and privacy is different, and the idea affects the content of the regulation.¹⁰ Especially, the definition of privacy is different thus privacy laws of each country are different. At the same time, the data is considered as a valuable asset to the economy, but the policies of the profiling regulations or anonymous data themselves are largely different and it might also cause the problems of utilising the space related data.

Each country's data privacy law is an inevitable part of regulation when we think of using space related data and the privacy.

Then, the question arises how we should think about Satellite Data in line with the data regulation.

9 Data protection regulation can be a key concept of utilizing the data, and the idea of using technology and data sometimes contradicts with the regulation. In the U.S., there is no general personal data protection law, on the contrary, EU has written a long privacy regulation bill.

10 COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, https://ec.europa.eu/info/sites/info/files/celex_32016d1250_en_txt.pdf (accessed on 15.1.2021).

Typical example to look at the different regulation could be EU's GDPR, California the United States' regulation, and Japan's personal data protection regulation.¹¹ GDPR, California Consumer Privacy Act of the U.S, and Japan's Act on the Protection of Personal Information, are all different. When we think of dealing with satellite data business and consumer protection, we need to cope up with the different level of protection by different countries and notions.

3.1. GDPR Declares the Protection of Personal Data as One of the Fundamental Rights

In April 2016, the EU adopted a new regulation on controlling the data which is called- the General Data Protection Regulation (GDPR). This new data protection regulation, GDPR went into effect on May 25, 2018. The new GDPR rules recognize the right to data portability and other rights of reference in other countries (Article 22 on forgotten rights, etc.).¹²

GDPR clearly sets the right to the protection of personal data as a fundamental rights, based on Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) that provide that everyone has the right to the protection of personal data.¹³

3.2. CCPA in Comparison

On the other hand, California's CCPA¹⁴ also grants California residents new rights regarding personal information. It is important because California holds leading high-technology companies including Google and Amazon etc. CCPA however regulates the companies that have gross revenue greater than 25 million, and annually shares or sells, buys, receives the personal information of 50,000 consumers. (GDPR regulates data controllers and data processors that are related to EU.) The scope and territorial reach is much greater in GDPR. Especially, the profiling regulation is completely different.

3.3. Personal Data Protection Law in Japan

In recent years in Japan, various regulations have been put in place regarding personal information in general, including reorganization into the Personal

11 The EU General Data Protection Regulation went into effect on May 25, 2018, replacing the Data Protection Directive 95/46/EC. Designed to increase data privacy for EU citizens. See 'The general data protection regulation applies in all Member States from 25 May 2018', <https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html> (accessed on 15.1.2021).

12 Ibid.

13 Ibid.

14 Andy Green, 'California Consumer Privacy Act (CCPA) Compliance Guide', <https://www.varonis.com/blog/how-varonis-helps-with-the-california-consumer-privacy-act-ccpa/> (accessed on 15.1.2021).

Information Protection Commission. The Act on the Protection of Personal Information revised in 2015, the Act on the Protection of Personal Information Held by Administrative Organs was revised in 2016, and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies came into full force on May 30, 2017.

3.4. Right to Object to Processing Data

Right to object to processing for profiling, direct marketing, and statistical, scientific, or historical research purposes is clearly written in the article 21 of GDPR, but it is not written in CCPR. There is a right to opt-out of personal information sales based on the civil code of California, but CCPA does not say anything about profiling regulation.

It is substantially different. Satellite data can be regarded as illegal when sold to companies for profiling, direct marketing, statistical, scientific research and the company does not clarify the right to object to the related data subjects.

Japan is regarded by EU to have equipped with sufficient data protection system, so Japan also requires consent by data subject for processing data.

3.5. Should Satellite Data be Regarded as Personal Data?

Specifically, there are limitations in the processing of satellite data. Particularly within the scope of application of the GDPR and the Japanese Personal Data Protection Act, the possibility of getting consent may be the most difficult part to overcome. Plus, the problem also occurs related to data profiling. Utilizing data means that profiling the data is sometimes necessary, however, if it is impossible to do so because the data cannot be combined with other related data.¹⁵

For example, if the movement of a car in the vicinity of a residence is detected by satellite, sales data of the car is obtained, but the profiling is required to identify an individual. Then, the question arises if it is possible to the data statistically. The movement of cars around the hospital may be sensitive data, but is such analysis also prohibited? How should we think of public figures like politicians?

Regarding satellite remote sensor, the direction of “Freedom to use remote sensor data” is shared internationally. Is it possible to interpret this by incorporating the idea into the data law and its regulation?

For example, the processing of satellite images corresponding to personal data is permitted in the case of responding to disasters and environmental problems already (for example, to identify perpetrators of environmental crimes). For example, if a disaster is impending in a remote area, and if the

15 Profiling is deeply concerned in privacy data protection regulation in Japan. See Mayu Terada, *Sentan Gijutsu to Kisei no Kōhōgaku* (Public Law on Advanced Technology and Regulation) (Tokyo, Keiso Shobo Publishing, 2020) [in Japanese].

resident is identified by matching with the residence information, it is immensely helpful. Thus, possible way to use satellite data is to issue an evacuation order and include such system internationally.

4. Solution in Practice

Solving the problem is more difficult than identifying the problem. While it is expected that the personal data law is applied to satellite data in a manner consistent with the space law, as discussed in 3.5, there is no guarantee that the regulators and courts of all the states will adopt the idea. Therefore, the industry has to find a solution by private arrangement.¹⁶ Such private arrangements may be designed on the basis of the current data transactions over platforms.

For example, the platform may require the data provider to guarantee that all the laws and regulations have been complied with when collecting the data and to transmit the requirements that the users of the provided data must respect. It will be something similar to the “representations and warranties” clause used in corporate and financial transactions. Under such terms of use of the platform, the provider of data shall be responsible, if the personal data law of some state has been breached in the process of collecting and transferring to the platform of the data and the user (or platform) suffers damages.

Based on such guarantee by the data provider, the platform may indicate the conditions for use regarding each piece or set of data.¹⁷ Then the user can trade such data by respecting the indicated conditions of use. If needed, the user may negotiate with the data provider to modify or derogate from the indicated conditions for use. Still, most users may simply choose the data, considering the indicated conditions for use as an element in making its choice. It will be useful if the conditions are indicated in a machine-readable manner as well, since the user of the data may wish to process the data without human intervention.

5. Conclusions

To conclude, the application of data law to the commercial satellite remote sensing should be made in a way that does not undermine the freedom of satellite remote sensing. Such freedom, covering both collection and use of data, is the principle established under the space law and developed through the global cooperation scheme. Furthermore, the aim of the data law is in the trusted use of data, not in limiting the use of data. This point was

16 Baumann & Pellander (fn 3).

17 Jordi Sandalinas, ‘Spatial Data Infrastructures for Marine Data Management’, 68 (2019) *ZLW*, pp.412-420.

pronounced in the Osaka Leader's Declaration at the G20 Summit in 2019 requesting the "free flow of data with trust".¹⁸ The practical solution will be to set up appropriate private arrangements through the platform. Still, it must be acknowledged that there remains a risk for the data users, as well as data providers. In the longer term, it will be needed to globally formulate and share the general ideas about the conditions and limits of the collection and use of satellite data, through dialogues with various stakeholders.

Acknowledgements

This paper is based on the research funded by the Japan Society for the Promotion of Science (JSPS), grant identifier 19K21678.

18 G20 Osaka Leaders Declaration, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html (accessed on 15.1.2021); G. Greenleaf, 'G20 Makes Declaration of 'Data Free Flow With Trust': Support and Dissent', [2019] 160 *Privacy Laws & Business International Report* 18-19.

