Earth observation applications and the right to privacy: within and beyond the COVID-19 pandemic

Shi, Y.

JURNAL MEDIA HUKUM
Vol. 29, No. 2, December 2022
P-ISSN: 0854-8919, E-ISSN: 2503-1023
Nationally Accredited Journal, Decree MoHE No. 148/M/KPT/2020.

Earth Observation Applications and the Right to Privacy: Within and Beyond the COVID-19 Pandemic

Yuran Shi
Leiden University, Netherlands
Corresonding Author: yuran.shi@outlook.com

ARTICLE INFO

Keywords:
COVID-19 pandemic; earth observation; privacy protection; privacy ranking regime; space law

How to cite:
Shi, Y. (2022). Earth Observation Applications and the Right to Privacy: Within and Beyond the COVID-19 Pandemic. *Jurnal Media Hukum, 29(2),* 107-119.

Article History:
Received: 06-04-2022
Reviewed: 08-08-2022
Revised: 13-08-2022
Accepted: 26-10-2022

ABSTRACT

Earth Observation (EO) applications interact with many industries and government practices. When EO applications touch upon data being able to identify individuals or certain groups, the processing methods adopted therein entail the balance between public interests in EO applications and the values of privacy protection. It then raises the question of whether and to what extent the EO data comes under privacy protection. This study builds on the methodologies of positive law analysis and normative analysis, with supplementary discussions on the role of EO applications in the COVID-19 pandemic. In recognising the conclusion that the right to privacy entails restrictions on data processing within EO applications, the principle of proportionality calls for solutions to fill the gaps in the regulatory framework. Though legislative solutions are possible in theory, it is not an easy job to get consensus among States in practice. A more appropriate solution lies in introducing a privacy ranking regime internationally, with supplementary enforcement practices on the regional and national levels.

DOI: https://doi.org/10.18196/jmh.v29i2.14435

1. Introduction

The EO refers to gathering information about planet Earth's physical, chemical, and biological systems via remote sensing technologies. Whilst, not all those activities are launched and targeted at people, the EO can collect identifiers and involve their processing and transfer among space activity operators. The issue of privacy protection increasingly raises regulatory concerns in the context of EO applications (Di Lullo, 2019).

The governmental restriction policies pertaining to the COVID-19 pandemic expose legal challenges arising out of privacy protection within EO applications (Satriawan & Seviyana, 2021). Struck by the COVID-19 pandemic, some States started resorting to Earth observation as a surveillance tool for predicting outbreaks, directing epidemic prevention policies, and helping understand the effects of COVID-19. Professor Rita R. Colwell from the University of Maryland has developed a predictive model for COVID-19 with the help of EO data (Broom,

2020). Satellite data helps measure population movement, constructions on the ground, and surface temperature. The information can be further used to predict outbreaks and help direct mitigation measures. ESA also issued two new initiatives related to understanding the effects of COVID-19 (ESA, 2020). Whilst sensitive data raises privacy infringement risks, the positive effects of satellite data on the prevention of COVID-19 spreading are noticeable, leading to legal challenges regarding the evaluation of legality, necessity, and proportionality of data processing practices within EO applications.

The development and deployment of LEO satellite constellations can also lead to regulatory concerns with respect to privacy infringement (Hofmann & Blount, 2018). Satellite technologies provide high-resolution images and videos, which make identification easier and more common. Space-borne data can be related to a specific individual. The main question pertaining to LEO satellite constellations is when and how the collection, processing, and distribution of satellite data are lawful in the context of privacy protection (Froehlich & Tăiatu, 2020).

In this connection, international law has not provided a satisfactory answer. As introduced by the UN General Assembly, the Remote Sensing Principles set out regulatory rules regarding remote sensing of the Earth from Outer Space. Whereas this regulatory instrument does not have legally binding effects on the States, it contains no provision addressing privacy protection in the context of EO applications. To this end, regulatory authorities must have recourse to interpretations of the Outer Space Treaty and international privacy protection laws. The regional regulations and national laws can also impact the right to privacy within EO applications in corresponding jurisdictions. Moreover, the particularities of satellite data distinguish legal challenges regarding privacy protection in EO applications from that in other sectors (Von der Dunk, 2009). General privacy protection rules shall apply *mutatis mutandis* to EO applications. This paper addresses whether and to what extent the right to privacy can be recognised under international law regarding satellite data within EO applications.

2. Method

This study builds on both positive law analysis and normative analysis. The positive law analysis is conducted through elaborating relevant legal instruments, inter alia, the Outer Space Treaty.[1] A thorough examination of international, regional, and national laws can provide positive law evidence on currently available legal instruments and is critical to understanding the pros and cons of existing. The normative analysis investigates the right to privacy, freedom, and remote sensing principles. The traditional theories for international space law, private international law, and international human rights law are examined in relation to whether they can be applied to issues concerning EO applications and how they can be coordinated during the implementation. The interpretation of these legal sources shall accord with the balance between public interests in EO applications and values of privacy protection (Georgiadou & Kounadi, 2020).

[1] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, henceforth referred to as the Outer Space Treaty.

3. Discussion and Analysis

3.1. Regulatory Framework Pertaining to EO Applications

3.1.1. How to Define the Relevance of Legal Instruments

It is not an easy job to analyse privacy issues within EO applications. There is no specific international treaty addressing legal challenges and perceived concerns therein. Proactive and flexible application of relevant legal instruments then becomes necessary. Privacy protection within EO applications is the overlapping field not only between the right to privacy protection and freedom of information but also between space law and data protection law (Blount, 2015).

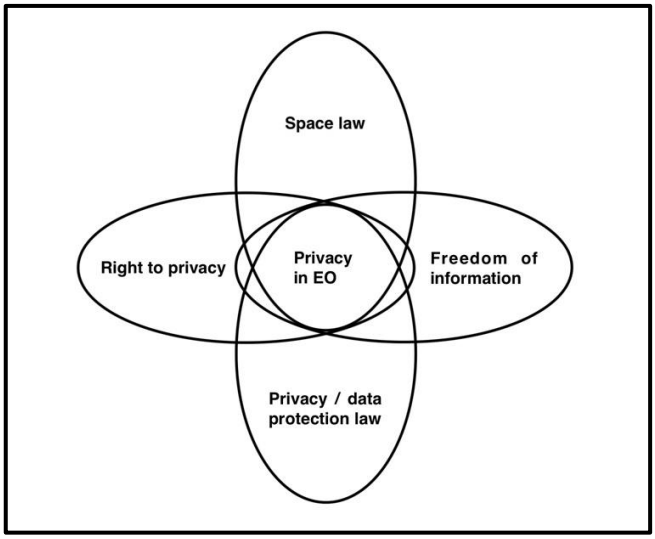

Figure 1 Legal elements concerning privacy issues in EO applications

With regulatory rules from various legal departments and on different levels, the establishment of a pragmatic and comprehensive framework requires the coordination of these legal instruments. This study will then explore statutory provisions related to privacy protection within EO applications.

3.1.2. Remote Sensing Principles as the Soft Law

The UN General Assembly introduced the Remote Sensing Principles. Based on the non-binding legal status, their implementation is left to the will of the States. Principle 1 provides definitions of some key terms. As mentioned above, the definition of remote sensing restricts the application of the principles to certain types of EO applications. This provision also provides the distinction between definitions of primary data, processed data, and analysed information. It facilitates the understanding of the nature and interaction of satellite data and human rights. Furthermore, principle 4 recognises the freedom of exploration and use of outer space on the basis of equality which has been established as the basic international space law principle through article 1 of the Outer Space Treaty.[2] With principle 6 encouraging

[2] Article 1 of the Outer Space Treaty: The exploration and use of outer space, including the moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind. Outer space, including the moon and other celestial bodies, shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies. There shall be freedom of scientific investigation

international cooperation on data collecting, storage, processing, and interpretation, principle 9 introduces data sharing obligations of States which have carried out remote sensing activities, as well as principles 10, 11, and 12, the Remote Sensing Principles establish and recognises the freedom of information. There is, however, no explicit provision regulating privacy issues within EO applications.

3.1.3. International Space Law and International Privacy Protection Law

Article 1 of the Outer Space Treaty establishes freedom in the exploration and use of outer space, based on which States are entitled to conduct EO activities without territory restrictions (Santos & Rapp, 2019). This provision also introduces the cooperation obligation, which can be regarded as the treaty basis of data-sharing clauses in the Remote Sensing Principles.

While there is no independent and comprehensive international treaty on privacy protection, international lawyers can find relevant traces in many international instruments. For instance, as a basic human right, the right to privacy is recognised and protected by international human rights law and European human rights law,[3] as well as case-law interpretations (Von der Dunk, 2009).

On regional and national levels, there are such data protection regulations established to solve relevant privacy issues as the GDPR for the EU Member States, article 6 of which reads as follows:

> Rapid technological developments and globalization have brought new challenges to the protection of personal data. […] technology has transformed both the economy and social life and should further facilitate the free flow of personal data within the Union and transfer to third countries and international organizations while ensuring a high level of protection of personal data.

Hence, data protection regulations provide important statutory support to solve privacy issues within EO applications. From a practical point of view, a provider of satellite-derived products or services is analogous to a data controller or data processor under GDPR (Von der Dunk, 2009). The hurdles of implementing these regulations lie in the particularities of satellite data, which distinguish EO applications from other processes related to personal data.

3.1.4. Selected State Practices in Respect of Privacy Protection

With respect to space-generated data and information, privacy is largely a domestic issue (Von der Dunk, 2013). The reading of national laws of, on the one hand, France and Germany as examples of civil law jurisdictions, and, on the other, the US as an example of common law jurisdiction, shows great similarity. The right to privacy is a fundamental human right

in outer space, including the moon and other celestial bodies, and States shall facilitate and encourage international co-operation in such investigation.

[3] Article 8 of the European Convention on Human Rights reads as follows: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

(Anggriawan et al., 2022). Article 9 of the France Civil Code sets out that everyone has the right to respect his private life. Some States introduced specific regulations on remote sensing, and there are rules concerning data control. However, most of these provisions cover data security issues on the governmental level, which are devoted to a different legal field from the privacy protection needs of individuals or certain groups. For example, article 17 of the Germany Satellite Data Security Act establishes the regime of sensitivity tests, while this regime is not about sensitive personal data. It is actually about national security and introduces some security measures to protect sensitive geographic data. The US and Canadian remote sensing regulations similarly introduced shutter control regimes (Bohlmann & Soucek, 2018). They address national security rather than personal data in EO applications (Froehlich & Tăiatu, 2020).

3.2. Personal Data in the Context of EO Applications

3.2.1. Delimitation of Personal Data

To get proper delimitation of personal data involved within EO applications, it is helpful to introduce a proper definition of Earth Observation first. As established by Remote Sensing Principles, remote sensing means sensing the Earth's surface from space by using the properties of electromagnetic waves emitted, reflected, or diffracted by the sensed objects to improve natural resources management, land use, and the protection of the environment. Considering that this definition was initially established for the application of the Principles, EO applications in practice probably present different features. Specifically, the purposes of these activities are not limited to natural resources and the environment (Froehlich & Tăiatu, 2020).

One of the important elements to delimitate personal data concerns identifiers, which can be used to identify individuals or groups (Taylor et al., 2016). Typical identifiers include physical features, contact information, location, and trajectory (Georgiadou et al., 2019). Under the freedom of information established by international space law, these identifiers might be collected, processed, or transferred among space activity operators (Aloisio, 2018).

Compared with early remote sensing imagery, which was not able to depict a person because of quite low resolutions, EO satellites nowadays reach a resolution high enough to depict specific individuals. In most cases, the law concerning privacy protection is, therefore, applicable to such data (Von der Dunk, 2021). This does not mean the resolutions allow for the identification of an individual by his or her face (Aloisio, 2018). Available resolutions of satellites, especially among civil and commercial sectors, cannot reach such a high level. There are two main ways in which EO data is able to identify individuals or certain groups. On the one hand, characteristics such as an individual's body type, height, and clothing can be used to identify the person. On the other hand, location, trajectory, and geographic information may be linked to individuals, either directly or combined with other information. For example, satellite imageries of a swimming pool or a house with a special garden can be linked to its owner and such data is regarded as personal.

Delimitation of personal data in EO applications is time-based, meaning that the identifiability of satellite data is decided with consideration of the state of art in technology. With the rapid development of satellite industries, operators shall consider the possibility of identification which can be accomplished after the data has been kept for several years (Froehlich & Tăiatu, 2020). In this context, the EO operators act as the data collector and must secure the consent of data subjects in cases of data collection as well as, if any, storage, processing, and transfer of personal data.

3.2.2. Incompatibility between Privacy and Freedom of Information

The right to privacy and the freedom of information are two fundamental elements concerning data protection in EO applications. On the one hand, the right to privacy is a basic human right. Take the EU as an example. Personal data issues increasingly gain attention from both legal and technical sides. The General Data Protection Regulation in the EU consists of a number of rules for the processing of personal data. As regards data protection legislation, the GDPR promotes global regulatory awareness of the right to privacy as a basic human right in the context of data protection. Though some EO applications are not targeted at individuals, the right to privacy still cannot be overlooked during these specific operations. On the other hand, freedom of information is broadly recognised in international space law and has brought many benefits in both commercial and non-commercial ways. Then one main challenge to solving privacy concerns in EO applications depends on weighing up privacy protection and freedom of information.

The right to privacy covers protection on both individual and group levels. If the trajectory and concentration of a certain group, like residents living in a certain area, is analysed and recorded, the religious belief and other sensitive information of this specific group are likely inferred therefrom (Nissenbaum, 2020). Personal data encounters the risk of being violated. This issue happens more frequently and is more serious in such *ad hoc* EO applications as surveillance policies during the COVID-19 pandemic. In this connection, sensitive information is then more likely involved, and certain groups might be exposed to unfair treatment in the future employment and bank loaning procedures on some inappropriate grounds, including the fact that they are from an outbreak zone or they have a blameable performance of governments' quarantine and mitigation policies.

Even if EO applications are focused on objects or a part of a property, they might capture information that can be linked to specific individuals accidentally. In this case, satellite data is recognised as personal data, regardless of the purposes of EO applications (Santos & Rapp, 2019).

3.3. Specific Challenges Arising out of Privacy Protection

3.3.1. Imperfection of Legal Framework

One of the reasons why privacy issues within EO applications are special lies in the fact that it is an overlapping field covered simultaneously by space law and data protection law (Masson-Zwaan & Hofmann, 2019). As mentioned above, though Remote Sensing Principles act as the basic legal instrument in the EO field, the definition of remote sensing included in principle 1 restricts the application of this resolution to certain purposes, such as environmental management. If remote sensing is sued for other purposes which are not covered by the principles, this fundamental regime is inapplicable. Furthermore, there is no international space law containing explicit stipulations about privacy protection in EO applications. Though some national laws or regional regulations introduced data protection rules on remote sensing activities, many of them focus on security issues. The issue of personal data protection within EO activities is actually an unregulated grey zone.

In other words, the responsibility of States established by OST for their activities does not result in any direct prohibition of the use of outer space for potentially interfering with privacy concerns on Earth (Von der Dunk, 2013). Article 6 of the Outer Space Treaty requires States to authorise and supervise relevant space activities. Thus, privacy issues in EO applications are more likely covered on the national level and regulated by domestic laws and regulations.

Also, because article 7 of the Outer Space Treaty and Liability Convention recognises the responsibility of the Contracting States, even for the damages caused by commercial sectors thereof, operators tend to base their corporations in States where licensing, privacy protection, and other relevant regulations are more friendly to them, like the recourse to 'flag of convenience' in maritime law. Such a situation is detrimental to privacy protection (Saboorian, 2019). Meanwhile, States, rather than individuals, are the parties to the Outer Space Treaty and Liability Convention, which means that individuals are not entitled to claim compensation on their own for the infringement of their privacy, increasing difficulties in privacy protection (Dodge, 2017).

3.3.2. Characteristics of Personal Data within EO Applications

Within the EO applications, personal data might be collected, processed, stored, and distributed, which is similar to data-related processes in other technological sectors. What differentiates the privacy issues within EO applications are some characteristics of the satellite data.

Firstly, to assess the possibility of identifying individuals based on EO data, stakeholders shall consider several objective factors, such as available tools for identification, the purpose pursued by the data controller, and the possibilities for technology development during the period for which the data will be processed. In many cases, satellite data are not collected for the purposes targeted at individuals, which causes considerable complexity to the question of whether such data can be recognised as personal data.

Secondly, the Outer Space Treaty contains provisions on information sharing, which create the duty of contracting States to notify other States of situations of impending disasters. EO applications are capable of collecting data about geographic and climate information, which is potentially covered by data-sharing duties (Oduntan, 2019). When these processes capture information related to individuals, geographic or meteorological data is much more likely transmuted into personal data, leading to the dilemma of contradictory privacy protection and data sharing obligations (Nhamo & Chikodzi, 2021).

Thirdly, different interpretations of data practices during EO applications are attributed to considerations of national security and privacy protection. For example, as the European flagship space program, the Copernicus is aimed at developing European information services based on non-space and EO satellite data. The technology provided by it has been used for EU border surveillance since early 2016 (Aloisio, 2018). One relevant issue is the refugee. What matters in space law is that the illegal immigration of people into Europe can be a security problem since people who immigrate in this way are neither controlled nor registered with local official authorities (Aloisio, 2018). Not only this, the border surveillance service provided by the Copernicus is also used for the investigation and prevention of international crime that is not necessarily related to illegal immigration (Froehlich & Tăiatu, 2020). The pressure brought by these issues is how much individual privacy the European citizens are ready to sacrifice for the supposed improvement of safety conditions, entailing the proportionality test of adopted EO applications.

3.3.3. Case Study: COVID-19 and EO Surveillance Programs

Data scientists and epidemiologists have collaborated to use newly available sources of digital data to track and predict outbreaks of disease (Fauziah, 2022). During the COVID-19 pandemic, tracking people through remote sensing has been a helpful tool in directing mitigation and quarantine policies (Masson-Zwaan, 2020). This is not the first case where

satellite data has been used for disease transmission control. Google Flu Trends model was designed to track flu infections using Google search records. Though it stopped publishing estimates of Flu and Dengue fever since 2015, it continues to provide relevant signal data to partners such as the Centres for Disease Control and Prevention (CDC) Influenza Division (Team, 2015). Data collection and processing still plays an important role in disease control and prevention.

There are also some algorithm models established to predict an outbreak of infection by using remote sensing data, such as the SARS-CoV-2 transmission model. The team has applied machine learning to data collected from China, Italy, Spain and the United States to extract correlations with data gathered from satellites, as well as surface parameters of moisture and ground temperature. In this process, personal data might be collected and processed, either intentionally or unintentionally. Even when satellite data does not necessarily identify individuals, it can be easily linked to certain groups, presenting risks of privacy infringements (Hofmann et al., 2018).

For some EO applications, people are not identified as individuals but as members of a specific group, and privacy protection shall then be owed to the group. The challenge here is that such privacy protection regulations are targeted at individuals rather than groups as the GDPR in the EU,[4] though in many cases, it is precisely being identified as part of a group which may make individuals most vulnerable. A broad sweep is harder to avoid than individual targeting (Taylor et al., 2016). When EO applications are used for tracking the population, it is possible to identify the dissident group that is holding meetings in a particular place or that an ethnic or religious group is targeted without specifically identifying individuals in the group. Thus, EO applications may be improperly used in ethnic or political violence. If the data released or distributed reflects the group and not specific individuals, threats can hardly be mitigated by data protection regulations or ethical standards. Meanwhile, legal issues of the data related to groups rather than individuals are also not easy to regulate with regards to invoking awareness of data subjects or receiving consent from them. Issues of subject consent on the group level are sufficiently addressed either in the technology industry or in academic research (Taylor et al., 2016). All in all, such usage of EO applications in disease transmission control touches upon the balance between the right to privacy and the benefits of surveillance on or predicting the newest situations of COVID-19 (Blount, 2017).

3.4. Possible Solutions to Privacy Protection Concerns

3.4.1. Privacy Ranking Regime of EO Applications

Stakeholders have proposed regulatory solutions to privacy protection issues concerning mobile phones (Liu, 2014). By building up a privacy ranking regime of mobile phone apps, domestic regulatory authorities supervise privacy policies of technology apps and direct relevant restriction policies on their download rates. This method can act as a valuable model for a privacy protection regime regarding EO applications while following two characteristics of EO activities call for appropriate amendments to this ranking regime (Chen et al., 2017).

[4] Article 1 of the GDPR reads as follows: [Subject-matter and objectives] This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

On the one hand, end users, or at least direct ones, of EO applications are normally not data subjects, which is a different situation compared with the market of mobile phone apps. For the latter, data subjects who care about privacy issues are also the users whose choice is vital to the development and expansion of companies. If a technology company does not have an admirable privacy policy or is troubled with data leakage accidents, it is likely in a disadvantaged position in the competitive market. Conversely, operators of EO applications do not necessarily need to gain popularity among data subjects since most end users of EO applications are governments, public organizations, or companies. Even in some cases, individuals make use of the processed data or analysed information from remote sensing activities, and they are not irreplaceable data subjects. Based on these reasons, the privacy protection conditions of EO operators are less important to end users and, consequently are less vital to operators.

Secondly, EO applications have considerable international elements. Based on the free use of outer space established by the Outer Space Treaty, EO applications with peaceful purposes shall not be restricted unless there are contrary treaty obligations against them. Furthermore, relevant data is more likely to be processed or distributed in a cross-border way (Schwartz, 2019). The ranking regime established by State A can hardly have legal implications in State B unless they have a bilateral agreement in place or establish judicial cooperation between them. National regulatory authority is thus not the best option to guide and supervise the ranking regime of transnational EO applications. To solve these two concerns, a ranking regime shall be established with the following principles observed.

Firstly, the ranking regime shall be established and pushed forward by neutral international organizations rather than domestic authorities (Von der Dunk, 2013), for which bilateral or multilateral agreements can provide applicable laws and institutional administration rules. An internationally universal ranking regime can have more practical values for privacy protection within EO applications compared with regulations within a geographically limited area.

Secondly, States shall be encouraged to take responsibility for privacy protection. With the ranking regime introduced, a legal question arises regarding whether it will have legal implications on domestic matters since it is not a legally binding regime. Only by being integrated into domestic statutory provisions or directly acting as binding international rules, the privacy ranking regime can truly lead to reforms on EO applications, either in technical or institutional spheres, with the inevitable loss of business interests of EO operators. Through such State practices as introducing national laws or recommended standards, the privacy ranking can play a role when end users choose remote sensing operators. For example, when using the data from an EO program with a high grade, the end user encounters fewer restrictions. And when using the data from the one with a low grade, such use might be limited or even restricted.

Thirdly, the privacy ranking regime shall recognise both main and relevant standards when rating the grades of EO operators to faithfully present privacy infringement risks. For example, EO applications can be rated based on three basic levels: applications with no privacy concern when there is no personal data collected, stored, processed, or distributed; privacy-friendly applications when only limited personal data is concerned, and most operations are not aimed at populations; privacy-invasive applications when there are sensitive personal data involved. These conditions are not absolute, and the final grade shall be decided with consideration of other relevant factors. For example, when EO operators actively carry out data protection and

privacy impact assessment policies or regularly conduct dialogues with manufacturers to implement privacy by design, their applications reasonably deserve a better grade whilst there is considerable personal data involved (Santos & Rapp, 2019).

Last but not least, it is indispensable to establish restriction and punishment policies as enforcement rules to facilitate the implementation of a privacy ranking regime, in which the duty of disclosure and extent of restrictions during the operation can be included. For example, if EO applications are rated as privacy-invasive, then the operators must publish conditions of data processing every three months and have to report to local regulatory authorities once they collect a certain amount of data (Bayamlıoğlu, 2018).[5] In some other instances, EO operators might be required to set up mechanisms to automatically process images by blurring images to filter out or obscure identifiable features (Santos & Rapp, 2019). Considering the difficulty for international organizations to independently implement these policies, national authorities or regional organizations like the EU shall take responsibility and proactively share relevant enforcement information with other States.

3.4.2. Interpretations of International Space Law

The solution regarding privacy protection in the EO applications is based on the rules of treaty interpretation, for which lawyers have to view international law as one legal system by using the method in article 31 of the Vienna Convention on the Law Treaties.[6] In other words, all these solutions shall aid the interpretation of international space treaties, especially the Outer Space Treaty thereof.

Article 7 of the Outer Space Treaty and the Liability Convention arguably build a comprehensive legal framework on liabilities of launching States for the damage caused by space activities to other States or natural and judicial persons (Von der Dunk, 2009). The core term 'damage' is defined by article 1 of the Liability Convention, which means loss of life, personal injury, or other impairment of health. It also includes loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations. In most cases, 'property' refers to tangible financial loss, such as buildings on the ground or satellites in outer space, considering the fact that drafters of the Liability Convention focused on the apportionment of damages and liability for satellite crashes (Saboorian, 2019).

However, if the damages of these two treaties are interpreted expansively to include incidents of privacy violations, relevant personal data issues can be covered by the space liability

[5] If implemented in the right context with ample instruments, transparency reduces the uncertainty and mitigates the effects of centralization, bias and information exclusivity.

[6] Article 31 reads as follows: [General rule of interpretation] 1.A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose. 2.The context for the purpose of the interpretation of a treaty shall comprise, in addition to the text, including its preamble and annexes: (a) any agreement relating to the treaty which was made between all the parties in connection with the conclusion of the treaty; (b) any instrument which was made by one or more parties in connection with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty. 3.There shall be taken into account, together with the context: (a) any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions; (b) any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation; (c) any relevant rules of international law applicable in the relations between the parties. 4.A special meaning shall be given to a term if it is established that the parties so intended.

framework. Amendments concerning data protection within EO applications can also be integrated into the Liability Convention based on article 25 thereof, referring to the amendment conditions. However, it is not easy to introduce such amendments because of the reluctance of States to reach a consensus on liability issues, which can be deduced from the limited number of States ratifying the Moon Agreement. Solving privacy protection issues within EO applications on the treaty level is not a straightforward task.

4. Conclusion

With the expansive development of EO applications, privacy protection issues have risen and continue leading to more regulatory concerns. If remote sensing is considered a service, the EU Member States are obliged to permit the EU providers of such services to offer remote sensing within their sovereignties on the same conditions as home-grown providers (Von der Dunk, 2009). The fewer restrictions faced by EO operators also mean more challenges to privacy protection. Still, any legal framework established for privacy protection shall acknowledge the necessity of processing personal data rather than denying it since such processes can benefit human beings through multiple uses of EO applications, such as tracking population in the mitigation of COVID-19.

When it comes to the question of whether the right to privacy deserves respect in the context of EO applications, the review of the international space law and data protection law validates the right to privacy to the extent that personal data protection does not compromise public interests within EO applications. To solve legal challenges and perceived concerns, such solutions as the privacy ranking regime can be helpful. Detailed instructions and standards shall be established on international, regional and national levels so that a comprehensive protection framework is introduced and properly administrated (Froehlich & Tăiatu, 2020). Only the privacy protection issues are to be solved well. EO applications are entitled to sustainable development in the future.

References

Aloisio, G. (2018). *Privacy and Data Protection Issues of the European Union Copernicus Border Surveillance Service*. Université du Luxembourg.

Anggriawan, R., Salim, A. A., Gunawan, Y., & Arumbinang, M. H. (2022). Passenger Name Record Data Protection under European Union and United States Agreement: Security over Privacy?. *Hasanuddin Law Review*, 8(2), 95-110. DOI: 10.20956/halrev.v8i2.2844

Bayamlıoğlu, E. (2018). Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation. *Available at SSRN 3097653*.

Blount, P. (2015). Remote Sensing Law: An Overview of Its Development and Its Trajectory in the Global Context. *Remotely Sensed Data Characterization, Classification, and Accuracies*, 639-656.

Blount, P. (2017). Seeing People: Using Satellites for the Benefit of All. *Proceedings of the International Institute of Space Law*.

Bohlmann, U., & Soucek, A. (2018). From 'Shutter Control' to 'Big Data': Trends in the Legal Treatment of Earth Observation Data. In *Satellite-Based Earth Observation* (pp. 185-196). Springer.

Broom, F. (2020). *Next COVID-19 Outbreak 'Predicted via Satellite'*. https://www.scidev.net/sub-saharan-africa/features/next-covid-19-outbreak-predicted-via-satellite-1/

Chen, L., Thombre, S., Järvinen, K., Lohan, E. S., Alén-Savikko, A., Leppäkoski, H., Bhuiyan, M. Z. H., Bu-Pasha, S., Ferrara, G. N., & Honkala, S. (2017). Robustness, Security and Privacy in Location-Based Services for Future LoT: A Survey. *IEEE Access*, *5*, 8956-8977.

Di Lullo, L. (2019). From Space to Earth: Assessing the Legal Framework of Big Data in the Space Technologies Sector. *Italian Association of Aeronautics and Astronautics XXV International Congress*.

Dodge, M. S. (2017). Assessing Refugee Crises through the Lens of the Outer Space Treaty and Space Technologies. *International Institute of Space Law*, *60* (Refugees and the Role of Space Communications: Status and Practice of the Charter for Man-Made Disasters), 351-362.

ESA. (2020). *COVID-19: How can Satellites Help?* https://www.esa.int/Applications/Observing_the_Earth/COVID-19_how_can_satellites_help

Fauziah, M. (2022). Urgency of Indonesia to Establish a Comprehensive COVID-19 Pandemic Law: Lesson Learned from Singapore. *Indonesian Comparative Law Review*, 4(1), 1-16. doi:https://doi.org/10.18196/iclr.v4i1.12999

Froehlich, A., & Tăiatu, C. M. (2020). *Space in Support of Human Rights* (Vol. 2). Springer.

Georgiadou, Y., de By, R. A., & Kounadi, O. (2019). Location Privacy in the Wake of the GDPR. *ISPRS international journal of geo-information*, *8*(3), 157.

Georgiadou, Y., & Kounadi, O. (2020). Digital Earth Ethics. In *Manual of Digital Earth* (pp. 785-810). Springer, Singapore.

Hofmann, M., Aloisio, G., & Rinaldis, L. (2018). Space-Based Services Supporting Refugees: Legal Aspects. *Proceedings of the International Institute of Space Law*, 363-376.

Hofmann, M., & Blount, P. J. L. M. (2018). Innovation in Outer Space: International and African Legal Perspective: 5th & 6th Luxembourg Workshops on Space and Satellite Communication Law. *Luxemburger Juristische Studien - Luxembourg Legal Studies* Baden-Baden.

Liu, Y. (2014). User Control of Personal Information Concerning Mobile-App: Notice and Consent? *Computer Law & Security Review*, *30*(5), 521-529.

Masson-Zwaan, T. (2020). Combating COVID-19: The Role of Space Law and Technology. *Air and Space Law*, *45*(Special issue).

Masson-Zwaan, T., & Hofmann, M. (2019). *Introduction to Space Law*. Kluwer Law International BV.

Nhamo, G., & Chikodzi, D. (2021). Use and Contestations of Earth Observation Technologies in Disaster Risk Reduction and Management. In *Cyclones in Southern Africa* (pp. 53-65). Springer.

Nissenbaum, H. (2020). Protecting Privacy in an Information Age: The Problem of Privacy in Public. In *The Ethics of Information Technologies* (pp. 141-178). Routledge.

Oduntan, G. (2019). Geospatial Sciences and Space Law: Legal Aspects of Earth Observation, Remote Sensing and Geoscientific Ground Investigations in Africa. *Geosciences*, *9*(4), 149.

Saboorian, A. (2019). A Brave New World: Using the Outer Space Treaty to Design International Data Protection Standards for Low-Earth Orbit Satellite Operators. *Journal of Air Law and Commerce*, *84*, 575.

Santos, C., & Rapp, L. (2019). Satellite Imagery, Very High-Resolution and Processing-Intensive Image Analysis: Potential Risks under the GDPR. *Air and Space Law*, *44*(3).

Satriawan, I., & Seviyana, D. (2021). Powers and Limits of State during COVID-19 Pandemic: a Critical Appraisal. *Yuridika*, 36(3), 663-692.

Schwartz, P. M. (2019). Global Data Privacy: The EU Way. *NYUL Rev.*, *94*, 771.

Taylor, L., Floridi, L., & Van der Sloot, B. (2016). *Group privacy: New challenges of data technologies* (Vol. 126). Springer.

Team, T. F. T. (2015). The Next Chapter for Flu Trends. https://ai.googleblog.com/2015/08/the-next-chapter-for-flu-trends.html

Von der Dunk, F. G. (2009). *Europe and the 'Resolution Revolution': 'European' Legal Approaches to Privacy and Their Relevance for Space Remote Sensing Activities*.

Von der Dunk, F. G. (2013). Outer Space Law Principles and Privacy. In D. Leung & R. Purdy (Eds.), *Evidence from Earth Observation Satellites: Emerging Legal Issues*.

Von der Dunk, F. G. (2021). Intellectual Property Rights as a Policy Tool for Earth Observation Data in Europe. In *Earth Observation Data Policy and Europe* (pp. 51-59). CRC Press.