


ATHENA

CRITICAL INQUIRIES IN LAW, PHILOSOPHY AND GLOBALIZATION

Globalization and AI Data Gathering in/from Outer Space: Building upon Lessons Learned at the European Level

ANTHI KOSKINA

*Professor of Law, IDEF College- Sorbonne Paris North University (Greece)
Research Associate, AthensPIL - National and Kapodistrian University of Athens (Greece)*

✉ akoskina@law.uoa.gr  <https://orcid.org/0000-0003-0896-1722>

KONSTANTINOS GALINAS

LL.M. Student, Democritus University of Thrace (Greece)

✉ kongali1@law.duth.gr

ABSTRACT

Based on the growing use of Artificial Intelligence (AI) –capable of gathering an unlimited (in amount and content) number of data, improving its functioning and simplifying tasks–, humanity appears to be in the midst of a fourth technological revolution. When such activity is conducted in outer space i.e., by fifth generation observation satellites (Fu W. et al. 2020) using AI, capabilities are strongly optimized; however, the activity also seems to pose serious threats to privacy and to industrial or national secrets. As a response to this challenge, AI data gathering on Earth is subject to specific frameworks protecting privacy, both at the upstream and downstream ends, such as in the case of the EU. Unfortunately, the rules established therein do not seem to be wholly applicable to AI data gathering in/from space, mainly due to the fundamental freedom to conduct space activity. As a choice must be made between competing interests, this article aims at discussing some of the elements that should be considered, when debating on a legal framework potentially applying to space AI data gathering; to avoid conduct of said activity only to the benefit of a few stakeholders against the background of an emerging regime of techno-feudalism.

Keywords: space law, artificial intelligence, satellite data collection, globalization of data, space policy

ATHENA

Volume 3.2/2023, pp. 37-79

Articles

ISSN 2724-6299 (Online)

<https://doi.org/10.6092/issn.2724-6299/17445>



1. Introduction

Described in general terms, globalization may be depicted as “the increasing worldwide integration of economic, cultural, political, religious, and social systems”¹, whereas it is usually likened to an invisible spider’s web covering the whole of the planet, on which strands “(p)eople, money, material goods, ideas, and even disease and devastation have traveled (...), in greater numbers and with greater speed than ever in the present age”.² At the same time, it is common knowledge that technological advances are at the heart of the globalization process, despite the fact that these may sometimes lead to negative effects.³ In this connection, attention is currently drawn to artificial intelligence (hereafter, AI), an innovative and even revolutionary technology, which allows for unprecedented opportunities for economic development.

In short, AI is based on the assumption that several aspects of human thought can be mechanized (Wasilow and Thorpe 2019, 37). Its most obvious feature – which separates it from earlier technologies – is the ability to act autonomously, without being bounded by the cognitive limitations of the human brain. It is expected that AI will soon be able to reach “*solutions that humans may not have considered, much less attempted to implement (...)*”⁴ whereas, up until now, such systems have provided effective solutions for numerous applications in all areas of everyday life, such as intensive care unit (Hanson and Marshall 2001, 427-428), petroleum exploration and production (Gharbi and Mansoori 2005, 94-95), and in the food industry (Kakani, Nguyen, Kumar, Kim, and Pasupuleti 2020, 6-9). Undeniably, the

¹ Globalization, *Oxford Reference*.

<https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095855259>.

² Globalization, *National Geographic Education*,

<https://education.nationalgeographic.org/resource/globalization>.

³ “The benefits and disadvantages of globalization are the subject of ongoing debate. The downside to globalization can be seen in the increased risk for the transmission of diseases like ebola or severe acute respiratory syndrome (SARS)”: Globalization, *National Geographic Education*. <https://education.nationalgeographic.org/resource/globalization/>.

⁴ “The AI’s solution thus may not have been foreseeable to a human, even the human that designed the AI” (Scherer 2016, 364).

development and commercialization of AI (i.e., artificial intelligence and machine learning processes) in combination with the extended use of information and telecommunication networks has accelerated the global economy, making it possible to utilize and synchronize complex data resources, financial flows and business processes (Sevalnev and Tsirin 2022, 379). In other words, AI allows for faster solutions to complex problems in all areas of the activity and the economy, through data gathering, processing and automated decision making (Iyer 2021,1).

Hence, since we are growingly using the data gathering and flow schemes produced by AI, one may argue we are living in the *era of digital globalization*: nowadays, globalization is being accelerated and redefined by said flows of data,⁵ whereas the use of AI techniques for data collection and processing is gaining in importance (e.g., as a significant tool for diffusion of knowledge and technology, as well as for enabling the distribution of production – of goods and services – across countries: Mattoo and Meltzer 2018, 770)⁶. In the context of global trade, the free and fast flow of data through AI systems can increase the benefits, provided that the “data transaction” remains trustworthy and the consumers do not face the risk that their data will be used for reasons beyond their knowledge or control.⁷ In practice, collecting and processing data via AI allows to reduce the time spent in operations, while accelerating the production of results.

Interestingly, each time such activities are carried out from space – in addition to allowing collecting a broader range of data (i.e., satellites may

⁵ Digital Globalization: The new era of global flows, *Mckinsey Global Institute*, <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-full-report.pdf> .

⁶ Meanwhile, the United States and many other nations (such as China, Israel, Singapore) are taking steps to ensure their competitiveness in AI in order to ensure their primacy from an economic and military perspective (Horowitz, Allen, Kania, and Scharre 2018, 8-9).

⁷ Policy Department for External Relations (Directorate General for External Policies of the Union), Two briefings and an in- depth analysis on Data flows, artificial intelligence and international trade : impacts and prospects for the value chains of the future (2020) [https://www.europarl.europa.eu/-RegData/etudes/IDAN/2020/653617/EXPO_IDA\(2020\)653617_EN.pdf](https://www.europarl.europa.eu/-RegData/etudes/IDAN/2020/653617/EXPO_IDA(2020)653617_EN.pdf).

gather data from all corners of the globe) which maximizes the use of AI –, these may benefit from a more flexible regulatory regime. In fact, satellite data gathering can be freely engaged in, pursuant to Article I of the Outer Space Treaty signed in 1967, which established the freedom to use outer space for peaceful purposes.⁸ Hence, up until now, two types of data-gathering activities may be conducted in/from space: Earth observation aimed at collecting information related to the planet's physical, chemical and/or biological features (Earth Observation/EO, or Remote Sensing/RS) or in reconnaissance activities, such as in the case of geospatial intelligence.

Nevertheless, no legal regime has been thus far established to specifically regulate the generation, use and/or protection of space big data (Von der Dunk 2013, 250). Regarding this particular field of activity, “space law is limited to the UN Remote Sensing Principles of 1986, which provide some general guidelines, but are of limited scope with regard to space big data. Moreover, laws on data and privacy protection, intellectual property and cyber security do not cover adequately the multi-faceted challenges presented” (Stefoudi 2017).

To clarify activities falling within each category, EO includes the currently popular Big Earth Data cloud processing platforms such as GEE,⁹ Amazon Web Services (AWS),¹⁰ Microsoft Azure,¹¹ NASA Earth Exchange (NEX),¹²

⁸ Art. 1 Outer Space Treaty 1967: “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”.

⁹ Google Earth Engine (GEE) is a cloud computing platform cloud that was launched by Google in 2010. It enables cloud computation and it is an effective tool for carrying out the analysis of global geospatial big data (Zhao, Yu, Li, Peng, Zhang, and Gong 2021, 2).

¹⁰ Amazon Web Services (AWS) as an application of cloud computing provide services in the following sectors: (a) security identity and compliance, (b) compute, (c) storage, (d) database, (e) migration, (f) media services, (g) machine learning, (h) Internet of Things (IoT) (Hashemipour and Maaruf 2020, 42-46).

¹¹ Microsoft Azure as an overarching brand name for Microsoft's cloud computing services and especially Microsoft Azure Machine Learning (ML) provide a rich set of algorithms that can be used to process huge amounts of data and design, test and deploy powerful and predictive analytics (Copeland, Soh, Puca, Manning, and Gollob 2015, 3).

¹² The NASA Earth Exchange (NEX) project is a collaborative platform that combines data access and computing capabilities in order to provide researchers with community supported modeling, analysis, visualization software and large-scale computing power in conjunction

Sentinel Hub (SH)¹³ and Open Data Cube (ODC)¹⁴ promoting the analysis and application of Big Earth Data, based on datasets acquired by EO satellites (Zhao, Yu, Du, Peng, Hao, Zhang, and Gong 2022, 1-3). At the same time, AI used for geospatial intelligence¹⁵ may allow to collect huge amounts of data which are both of a non-critical and/or confidential nature (e.g., relating to States' infrastructure, communication, military activities etc.) (Soroka and Kurkova 2019, 131-134). Seen from this angle, data gathering using AI in space may be used as a means for unlimited access to information, disregarding national boundaries or secrecy, as well as personal privacy.

Be that as it may, growing awareness of the potential of AI data gathering also led to the emergence of concerns regarding privacy rights and privacy issues (namely, private and/or non-private data protection). Indeed, while RS may be regarded as inoffensive, collecting and processing other types of data – e.g., related to critical infrastructure, military activities or even citizens – through space could well result in violations; e.g., violations of fundamental human rights of that country's citizens, like the right to privacy (UDHR, Article 12)¹⁶ and the principle of non-discrimination (UDHR, Article 2)¹⁷.

with datasets that are common to Earth systems science domain (Huffer, Cotnoir, and Gleason 2015, 2177-2180).

¹³ Sentinel Hub (SH) as a platform developed by Sinergise provides data access through certain OGC protocols, data processing and visualization services (Gomes, Queiroz, and Ferreira 2020, 5-6).

¹⁴ Open Data Cube (ODC) is an open and freely accessible data exploitation architecture that has a potential to face the new data management and analysis challenges from the huge increase in data volumes about Earth Observation (Killough 2018, 8629).

¹⁵By the term "geospatial intelligence" we consider all aspects of geospatial data processing including intelligent methods and technologies to fuse/integrate data and products acquired by multiple heterogeneous sources using machine learning techniques and emerging big data and geoinformation technologies (Kussul, Shelestov, Basarab, Shakun, Kussul, and Lavreniuk 2015,2).

¹⁶Art. 12 UDHR 1948: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".

¹⁷Art. 2 UDHR 1948: "Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional, or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty".

Furthermore, the same activity, carried out on a regular basis, could well raise the question of whether it is in line with the general principle of non-intervention, established in the Declaration on the Inadmissibility of Intervention and Interference in the Internal affairs of States, signed in 1965¹⁸ [still, given the “soft law” nature of the above instruments, there would be no breach of an international obligation – e.g., in case of a violation of individuals’ privacy –, hence no international responsibility; this is the reason why scholars suggest that with respect to space-generated data and information, privacy is very much a national matter, to be addressed by domestic (hard) laws and regulations (Von der Dunk 2013, 245)].

As a result, the principal question arising is whether AI data gathering, which is a vital instrument and a major tool for pushing globalization, should be regulated in a harmonized and legally binding way when conducted in/from outer space – as it is regulated when conducted on Earth –, especially taking into account that AI data gathering is optimized when conducted from space (and is, therefore, offering increased possibilities for continued globalization). In reality, ensuring the proper use of AI in space, in accordance with the OST and international law – including the Charter of the United Nations (as laid down in the Art. III of the OST) and the principles established therein¹⁹ –, is a challenge *per se*.

Against this background, this article aims at presenting first limits that were established as regards massive data gathering activities carried out via AI on Earth, on the basis of the EU data framework paradigm (Section 2). Subsequently, the unique issues resulting from the use of AI in space for the

¹⁸ RES 2131(XX), Declaration on the inadmissibility of intervention in the domestic affairs of states and the protection of their independence and sovereignty. This principle is additionally linked to espionage, which is defined as the effort to discover the guarded secrets of another entity using concealed and clandestine methods (Nickolas 2019, 29-32). In truth, espionage or reconnaissance techniques are not traditionally regarded as a violation of international law. However, a “growing body of national decisions has steadily recognized that territorially intrusive forms of espionage violate the principle of territorial sovereignty (Baker 2003, 1091-1096; Navarrete and Buchan 2019, 898-905).

¹⁹ The Charter goes on to envision a democracy of states that emanates from the founders’ faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small (Joyner 1999, 337).

purpose of data collection will be investigated, so as to define the problems encountered in the space environment (Section 3). The purpose of this article is to discuss possible solutions and approaches to ensure privacy protection, in the event of data gathering conducted via AI from/in space, as these will have to be addressed by policy makers (Section 4) and to formulate conclusions (Section 5).

2. Massive (AI) Data Gathering on Earth: Existing Approaches and Limits

It is difficult to know when the practice of large-scale data gathering really started. Be that as it may, the massive gathering of data gained ground recently in the context of administrative and judicial proceedings *inter alia*, and raised key concerns right from the outset. As this activity is mostly carried out through the use of AI, specific pieces of legislations and mechanisms were put in place to safeguard important human rights, such as privacy. In short, the growing use of robotics and/or AI, as well as their potential (negative) effects on citizens' privacy (Butterworth 2018, 258-264), is now widely regulated by Data Protection laws.

To name but a few examples, both US federal and State laws established a data protection policy in specific domains, such as the Health Insurance Portability and Accountability Act (HIPAA) or the Family Educational Rights and Privacy Act (FERPA) (Klosowski 2021). Similarly, the Australian Privacy Principles (APPs) of the Privacy Act 1988 established rules applying to the collection, use and correction of personal data (Zeller, Trakman, Walters, Rosadi 2019, 32-33). In this context, we suggest to focus and examine the EU data protection framework, considered sufficient to provide an overview of the issues at stake.

2.1 Protection of Private Data: The Case of the EU Data Protection Framework

In European Union law (EU law)²⁰, a milestone was reached in 2016, with the adoption of the General Data Protection Regulation (GDPR)²¹, regarded as more than a simple revision of the previous Data Protection Directive and less than a regulatory paradigm shift. More precisely, the GDPR regulates large scale data gathering, in the form of AI data collection (Ishii 2019, 515-517), when such process is related to individuals (Mitrou 2018, 32-33). Exceptions to the application of the GDPR are addressed in Section 5, Article 23 entitled “Restrictions”, to take account of the need to safeguard *inter alia* national security and defense. Thus, it may be concluded by an *argumentum a contrario*, that each time the requirements of Article 23 are not met, the GDPR shall apply.

More precisely, private data may first be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”, as established in Art. 5 of the GDPR; Art. 6 lays down that such personal data can be processed only following a clear and informed²² consent of the individual. In fact, such processing is lawful only if “the data subject has given consent to the processing of his or her personal data for one or more specific purposes” and/or “to protect the vital interests of the data subject”. Hence, the GDPR lays down rigorous conditions for the processing,²³ while use of data – namely, data collected and processed by AI – ought to be in line with the principle of non-discrimination (Charter of Fundamental Rights EU, Art. 21)²⁴. In addition, “[t]he data subject shall

²⁰ This analysis will draw on the paradigm of the EU data protection regime.

²¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

²² Article 13 of the GPDR.

²³ The processing shall be laid down by EU law or member state law, on the basis of Art. 6.3 of the GDPR.

²⁴ For example, the use of algorithmic profiling for the allocation of resources is, in a certain sense, inherently discriminatory (Goodman and Flaxman 2017, 53-55). Some governments

have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning it or similarly significantly affects it. In essence, this guarantees the right of the individual not to be subject to a decision based solely on an automated data procedure, with the exceptions referred to in paragraph 2”, pursuant to Article 22(1) of the GDPR.

Secondly, it is mentioned that such activity is lawful in case “processing is necessary *for the performance of a task carried out in the public interest* or in the exercise of official authority vested in the controller” (GDPR, Art. 6; emphasis added), whereas Art. 23 lays down that the protection of personal rights may be restricted for specific reasons, such as for national security reasons.²⁵ In any case, the conditions of necessity – based on the EU Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 8 (2) – and proportionality (see EU Charter of Fundamental Rights, Art. 52) need to be fulfilled.

More precisely regarding the necessity to restrict a human right, the EU Court of Human Rights has ruled that: “‘*necessary*’ (is) not synonymous with indispensable (...) neither has it the flexibility of such expressions as admissible, ordinary, useful, reasonable or desirable”.²⁶ Correspondingly, the principle of *proportionality* was fully developed by the European Court of Justice (ECJ) in the case *Internationale Handelsgesellschaft*,²⁷ where the Court underlined that the means chosen must meet a proportionality test

are already using algorithmic systems to classify people based on problematic categories (Latonero 2018, 11).

²⁵ Both the European Court of Human Rights (*Case of Big Brother Watch and Others V. United Kingdom* [GC], no. 58170/13,62322/14,24960/15, §274 -276, ECHR, 2021), the European Court of Justice (Case 623/17 *Privacy International V Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Services, Secret Intelligence Service* [2020] ECR) and the German Federal Constitutional Court, (BVerfG, Judgment of the First Senate of 19 May 2020 – 1 BvR 2835/17) had decided in favor of a legislation on the use of bulk communications data for security reasons.

²⁶ *Handy side v United Kingdom* App No 5493/72 (ECtHR, 7 December 1976); emphasis added.

²⁷ Case 11/70 *Internationale Handelsgesellschaft vs. Einfuhr und Vorratsstelle für Getriebe und Futtermittel* [1970] ECR 1125.

consisting of three components: (i) appropriateness, as the measure must be appropriate or suitable to protect the interests that require protection; (ii) necessity, meaning that no measure less restrictive must be available to attain the objective pursued; and (iii) proportionality *stricto sensu*, in the sense that the restriction must not be disproportionate to the intended objective or result to be achieved (Milaj 2016, 116-121) (up until now, the ECJ has issued a significant number of decisions interpreting the concepts of proportionality²⁸ and necessity²⁹ in the context of personal data restrictions, that may be taken into account).

On this basis, it appears that collecting and processing personal data may be conducted either following a prior, free, informed and express consent of the person(s) concerned, or for specific reasons of public and/or national interest, within the bounds of data protection and general international law (e.g., in line with the principles of necessity and proportionality). Theoretically, any violation of privacy and of a fundamental data-protection principle could be addressed in the courts, *inter alia* on the basis of Art.12 of the UDHR, taking furthermore into consideration that Art. 2 of Resolution 53/144 dated 9 December 1988 reads that “[e]ach State has a prime responsibility and duty to protect, promote and implement all human rights and fundamental freedoms...as well as the legal guarantees required to ensure that all persons under its jurisdiction, individually and in association with others, are able to enjoy all those rights and freedoms in practice”.³⁰ Thus, States must ensure the protection of citizens’ privacy as a fundamental human right, acting against any violation of their personal data as secured in the GPDR.

²⁸ Joined Cases C-465/00, C-138/01, and C-139/01 *Osterreichischer Rundfunk* [2003] ECR I-6041, Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971.

²⁹ Case C-524/06 *Huber* [2008] ECR I-9705.

³⁰ A/RES/53/144 Declaration on the Right and Responsibility of Individuals, Groups, and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms.

In addition to that, according to the International Covenant on Civil and Political Rights General Comment 16 (1988)³¹:

The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law... In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

Interestingly, though, the European Commission proposal for an EU regulatory framework on Artificial Intelligence (COM (2021)206 - 21.04.2021) regulated AI data processing, by suggesting a particular differentiation between ‘AI systems’ and ‘high-risk AI systems’; said approach implied that AI systems which do not interact with humans, are not used to detect emotions or determine association with (social) categories based on biometric data or that do not generate and/or manipulate such content, are eventually harmless. On the other hand, it was also proposed – in the Report of the European Parliament (Report A9-0001/2021 - 04.01.2021³²) on the military aspects of the use of AI –, that AI used in a military context “must be subject to meaningful human control, so that at all times a human has the means to correct, halt or disable it in the event of unforeseen behavior,

³¹ UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988.

³²European Parliament, Report A9-0001/2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)).

accidental intervention, cyber-attacks or interference by third parties with AI-based technology or where third parties acquire such technology”, and in all circumstances used in line with international public law, in particular humanitarian law.

Hence, based on the EU paradigm, it appears that a detailed framework was established to oversee the collection, processing and exploitation of private data, even when the public interest is at stake. In other words, massive data gathering conducted within the context of said States is strictly regulated, as such data refer to “identified or identifiable *natural persons*”: *they consist in sensitive data requiring special protection*. On this basis, the major role was given – for the specific purpose of private data protection – to the individual(s)’ consent and authorization.

2.2 *Defining the Importance and Role of the Individual’s Consent*

The fundamental principle of individual’s informed consent, as established in Art. 7 of the GDPR, is one of the best-known legal bases for processing personal data.³³ The basic requirements for a valid legal consent are defined in Art. 7 of the GDPR and specified in recital 32 of the GDPR. According to these provisions, individual’s consent must be freely given, specific, informed, auditable and unambiguous (Breen, Quazzane and Patel 2020, 22). It is noteworthy that the notion of a “free” consent implies the absence of any kind of inappropriate pressure or influence, while an informed consent “can be said to have been given based upon a clear appreciation and understanding of the facts, implications and consequences of an action” (Politou, Alepis, and Patsakis 2018, 6).

However, in case of any secondary uses of personal data for research (widely referred to as *derivative data*), the potential acceptance of a “broad consent” arises new challenges. Recital 33 of the GDPR states that “it is often not possible to fully identify the purpose of personal data processing for

³³As described in Art.6 (1) of the GDPR, the other legal bases are: contract, legal obligations, vital interests of the data subject, public interest and legitimate interest.

scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose”.

At the same time, according to Art. 29 of the GDPR Working Party Guidelines on consent under Regulation 2016/679:

it should be noted that Recital 33 does not disapply the obligations with regard to the requirement of specific consent. This means that, in principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, Recital 33 allows as an exception that the purpose may be described at a more general level (...) When regarded as a whole, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked.³⁴

Hence, it is apparent that the notion of “specific consent” remains a fundamental legal requirement for private data protection in both events; namely in case of the initial collection and processing of data, as well as in case of any secondary operations on said data.

Interestingly, Butterworth (2018, 261) underlines – in reference to big data processing – that:

if the purposes of the data collection and analysis are unclear when data are collected, it makes it difficult to obtain meaningful consent as required by the GDPR: “freely given, specific, informed and an

³⁴Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, p.28, <https://ec.europa.eu/newsroom/article29/items/623051>.

unambiguous indication of the data subject's wishes". Consent will also be difficult to obtain (or re-obtain) where data is observed rather than directly provided by data subjects, as in this context it is unlikely that data subjects will provide the "clear, affirmative action" required by Article 4 (11).

In theory, pursuant to Art. 7(3) of the GDPR, all data subjects retain the right to withdraw their consent at any time. Thus, once such consent is withdrawn, individuals have the right to have their personal data erased and no longer used for processing (Maldoff 2016). However, in the case of deep learning and data processing, the withdrawal of consent coupled by the continuation of learning through processing, would constitute a violation of the GDPR. Seen from this perspective, scholars suggest that: "it is likely that the GDPR provision will result in either large scale AI regression or continual liability risks for those continuing to derive learning from unlawfully processed information" (Humerick 2018, 407).

Overall, the massive (AI) collection and processing of data is regulated in detail when it is carried out on Earth – namely at States level –, providing a minimum level of protection to individuals against human rights abuses. However, said activity is also being conducted in space, using infrastructure and equipment which is placed in this particular environment, such as satellites in orbit around the Earth. Data gathering activities conducted in this specific manner are subject to completely different rules that are worth being considered, especially taking into account that in case AI is being used, the storage and/or processing and/or use of data for a variety of purposes, will be further optimized.

3. Massive (AI) Data Gathering from Space: Different Context and Issues at Stake

Massive (AI) data gathering conducted from space mainly consists of RS (or EO). To put things into context, RS is used to collect information on a wide

range of elements related to our planet, and for observing the Earth surface – as well as its weather and climate (Kumar, Arivazhagan, and Rangarajan 2013, 93-95) – while allowing to monitor numerous activities, like farming, agriculture (Weiss, Jacob, and Duveiller 2020, 2-3), fishing etc.

In recent years, RS has been revolutionized by AI (Gevaert 2022, 1-2). More precisely, since the mid-1950s, – when it was first developed as a branch of computer science –, AI marked significant growth rates, as it allowed to solve problems by using systems reproducing human intelligence features. In fact, AI’s first key technological purpose was to mimic human intelligence, rather than to function as a copy of it (Martinez 2019, 1024). However, it developed into a “goal-oriented, problem-solving thinking process, with at least some human-level (or better) capabilities” (Abney 2020, 65) embodied by machine learning based on data; the continuing improvement of deep learning systems attracted public attention, and gave private companies the opportunity to use a ground-breaking technology while prompting State regulatory bodies to enact better adapted rules (Wang 2019, 2). As a result, AI was also used to full advantage in the context of space activity: regarding *inter alia* RS, AI allowed to collect increasingly accurate and reliable information – with the use of on-board advanced techniques such as the “change detection” method³⁵ –, in order to treat it automatically and without any human intervention.

Interestingly – and this feature may be regarded, from a certain angle, as a disadvantage –, RS does not initially (i.e., during data collection) distinguish between the types and significance of data: an *a priori* differentiation between public and private data is not possible for technical reasons, given that RS mainly consists in “photographs” taken from space objects. As a result, a religious site will be detectable, just as easily as a farm or a military activity.

³⁵ For example, in the specific context of data gathering and processing from satellites in outer space AI techniques offer the possibility to select only the data of interest for a specific application or to extract accurate information from specific data. Applying this technique an AI satellite can use applications such as “change detection” for on-board data processing in order to store and send to the ground only the useful images e.tc. for the specific activity (Guerrisi, Del Frate, and Schiavon 2022, 2-3).

Hence, as RS may not be controlled in terms of the data being collected, questions seem to be raised as regards the massive data gathering from space, especially in the event that AI and AI processing are involved.

3.1 (AI) Data Gathering and Space: Inapplicability of the Distinction Private-public Data

Nowadays, space technology allows to remotely observe and monitor the planet, namely to capture the overall image of the Earth. In essence, RS is one of the oldest, most basic and essential activities, which may be defined as “a methodology to assist in characterizing the nature and/or condition or phenomena on, above or below the earth’s surface by means of observation and measurements from space platforms; at present such methods depend on the emission and reflection of electromagnetic radiation”.³⁶

In reality, for practical and economic reasons, the technology which is being used for gathering data from space is dual-use: namely, in this specific environment, a single space object may in principle be used for both civilian and military³⁷ purposes (i.e., without that being the result of a malfunction). Hence, the same space technology may be used to collect all types of data, without having to overcome any administrative or other obstacles, and without (technically) requiring any consent for the collection of data. On this basis, the differentiation between private and public data appears – at first – to be meaningless as far as data gathering from space is concerned; and more importantly, said technology may theoretically be utilized to intentionally harm others, or in an imprudent or self-destructive way (Gabriel 2020, 412).

³⁶ Definition used in the Draft Report of U.N. Working Group on remote sensing of the earth by satellites, 2nd session, 8 February 1973, U.N. Doc. A/AC 105/C1/WG4/L4.

³⁷ The role of AI in future military applications consists a matter of great concern. For example, the utilization of artificial intelligence technologies during warfare, such as fully autonomous weapons, LAWs or killer robots, underscore serious moral and legal concerns, mainly due to their capacity to select and engage their target without human control. Legal discussions also focus on the capacity of autonomous weapons to comply with fundamental principles of international humanitarian law, such as the principles of distinction, necessity and proportionality (Martin and Freeland 2021, 3-5).

Legally, data-gathering activities from space are governed by the rules of international space law, and especially by the Outer Space Treaty (hereafter, OST). Thus, account must be taken of Articles I-III of the OST laying down the freedom of States to conduct space activities³⁸ in general, in line with international law and the common aim of ensuring peace and promoting security and mutual cooperation,³⁹ and in conjunction with Article VI of the OST establishing the principle of the international responsibility of States with regard to their actions in carrying out their space activities.⁴⁰

Yet, given the particular importance of this activity, RS was additionally regulated by more specific rules, namely by the *UN Remote Sensing Principles*,⁴¹ established under UN Resolution 41/65 of 1986.⁴² More precisely, according to said principles, a basic distinction was made between three categories of data depending on the degree of processing applying to them: “primary data”, “processed data” and “analyzed information”⁴³ (Principle I).

In practice, this categorization has certainly served as a reference for space policy-makers and space practitioners in a few States, despite the fact that

³⁸ OST, Art. I (3): “There shall be freedom of scientific investigation in outer space ... and States facilitate and encourage international co-operation in such investigation”.

³⁹ OST, Art. III: “States Parties to the Treaty shall carry on activities in the exploration and use of outer space (...) in accordance with international law (...) in the interest of maintaining international peace and security and promoting international co-operation”.

⁴⁰ OST, Art. VI: “States Parties to the Treaty shall bear international responsibility for national activities in outer space (...) whether such activities are carried on by governmental agencies or by non-governmental entities (...)”.

⁴¹ It should be noted that the term “remote sensing” is often used interchangeably with the term “earth observation”.

⁴² Principles Relating to Remote Sensing of the Earth from Outer Space, G.A. Res. 41/65, U.N. Doc. A/RES/41/65(Dec. 3,1965), (thereafter Res. 41/65). UN Resolution 41/65 is not binding. However, as domestic laws have “regularly deferred to Resolution 41/65”, its principles are generally perceived to constitute customary international law (Von der Dunk 2009, 417). Be that as it may, most authors underline the non-binding nature of Resolution 41/65. More specifically, Lyall and Larsen (2017, 370) argue that “it still seems to us premature to suggest that in toto the UN Remote Sensing Principles constitute customary international law; they may be soft law, and it is true that states which have not adopted national legislation have only the UN Principles and general international space law as their guide”.

⁴³ Art. I Res. 41/65: “(b) “primary data” means those raw data that are acquired by remote sensors borne by a space object (...); (c) “processed data” means the products resulting from the processing of the primary data (...); (d) “analyzed information” means the information resulting from the interpretation of processed data”.

national approaches to precisely defining RS data sometimes diverge (Doldirina 2015, 75). For example, the US Land Remote Sensing Policy Act adopted a similar distinction between data and information – i.e., depending on the processing applied –, and defined EO as an activity aimed at the ‘collection of data which can be processed into imagery of surface features of the Earth’.⁴⁴ On the contrary, the German Satellite Data Security Act (SatDSiG) released in 2007, and the Satellite Data Security Ordinance (SatDSiV) of 2008, negated the importance of the distinction between raw and processed data, or information, by defining EO data as “signals of satellite sensors and all products derived from them, notwithstanding the level of processing and the mode of their storage and presentation” (Doldirina 2015, 75).

Hence, it appears that international space law has not – up to now – addressed the topic of data gathered from space in a holistic and comprehensive manner, taking into account all the issues at stake. On the one hand, it does not regulate potential violations of individuals’ right to privacy [the OST does not provide much specific guidance about addressing possible privacy concerns (Von der Dunk 2013, 245)] neither do the other international law rules applicable to space activity on the basis of the OST (e.g., the UN Charter mainly considers gross-scale violations of human rights: *ibidem*). On the other hand, the issue of data related to the natural resources of States were hotly debated early enough, showing in truth that the positions of States substantially diverged. More precisely, the dichotomy – underlying much of Resolution 41/65 – was between States which feared that other States’ RS activities would encroach upon their permanent sovereignty (especially in the context of natural resources) namely sensed States, and States wishing to access the data (Von der Dunk 2013, 417). Thus, Latin American nations argued that the sovereignty over their natural resources should be combined with the sovereignty over the data concerning those resources gathered via

⁴⁴ H.R. 6133 – Land Remote Sensing Policy Act 1992.

RS operations; contrary to that, the United States opposed a consent-driven position, arguing that Art. I of the OST established absolute freedom in outer space (Sinha 2012, 253).

The result was that Principle XII of Res.41/65⁴⁵ established no strict obligation of the sensing State to request the “prior consent” of the sensed State before passing over it and monitoring its territory (Bohlmann and Soucek 2018, 187). Hence, the issue was addressed in a pragmatic and realistic way, as it was argued that sovereignty may be regarded as “almost meaningless if other states obtain superior quality information regarding the developing state’s territory and the resources therein” (Von der Dunk 2009, 417). In this context, one may as well argue that the question of the consent or authorization of the sensed subject (i.e., of States and/or possibly of persons) to data collection and processing was not addressed in a fully satisfactory manner;⁴⁶ and this position has not changed despite the fact that data-gathering activities from outer space (namely EO or RS) are being more complex and intrusive, given that they are growingly based on the use of AI systems in space.

Be that as it may, RS activities have now led to the creation of important data bases, making the most effective use of information-gathering space technology. By way of illustration, massive public data gathering activities – requiring enhanced collaboration within a context of ever-accelerating globalization – resulted on the creation of the *Group on Earth Observations* (GEO) as a voluntary partnership of more than 100 national governments and in excess of 100 participants Organizations aimed at achieving the operation

⁴⁵ Art. XII Res.41/65: “the sensed State shall have access to them on a non-discriminatory basis and on reasonable cost terms. The sensed State shall also have access to the available analyzed information concerning the territory under its jurisdiction in the possession of any State”.

⁴⁶ Arguably, the perspective of the protection of personal data and privacy could then have been discussed, given that: “when the space law era was ushered in during the late 1950s, it was already clear to some observers that, sooner or later, life on Earth, would be monitored from a distance without those living on it necessarily knowing about it – Big Brother in *optima forma*” (Von der Dunk 2013, 243).

of a *Global Earth Observation System of Systems (GEOSS)*⁴⁷: that is, a set of coordinated, independent EO, information and processing systems that interact and provide access to diverse information for a great number of users while governed by the principles of openness,⁴⁸ effectiveness,⁴⁹ flexibility,⁵⁰ sustainability⁵¹ and reliability.⁵²

Overall, GEOSS was implemented as a global hub for EO allowing to collect relevant data and information and is currently regarded as a platform aimed at “easing discovery and access to the many datasets made available by national and international organizations” (Boldrini, Nativi, Hradec, Santoro, Mazzeti, and Craglia 2023, 716). Therefore, taking into account the undisputable success and utility of this initiative, the question arises as to whether it would be opportune to propose conditions and limits to massive (AI) data gathering from space – and to regulate and respond to what precise sorts of threats – as an *a priori* rule.

3.2 Threats Posed by AI in the Context of RS: Optimization Without any Limits

A key feature to the RS activities as carried out today is that advances in spatial resolution have been coupled with advances in image processing (i.e., through AI data processing algorithms) providing new research possibilities. The continued progress in satellite RS and the initiative of building next-

⁴⁷ More info on GEO and GEOSS available on https://www.earthobservations.org/geo_community.php

⁴⁸ Openness: The architecture shall be open and allow interoperability among multiple stakeholders to contribute their data and services and add value to the GEOSS, GEO Strategic Plan 2016-2025: Implementing GEOSS, in https://www.earthobservations.org/documents/open_eo_data/GEO_Strategic_Plan_2016_2025_Implementing_GEOSS_Reference_Document.pdf.

⁴⁹ Effectiveness: The architecture shall be capable of sufficient performance in all areas to support the Strategic Objectives of GEO in the implementation of GEOSS (*ibidem*).

⁵⁰ Flexibility: The architecture shall be scalable, to meet current and future requirements; flexible, to meet a broad variety and scale of GEOSS requirements; and agile, to be able to provide solutions across GEOSS with minimum tailoring and re-architecture (*ibidem*).

⁵¹ Sustainability: The architecture shall provide the solution for the near and long term in a cost-efficient manner, as technology, policies, and data providers change (*ibidem*).

⁵² Reliability: The architecture shall be robust and allow GEOSS to meet users’ expectations and effectively manage risk (*ibidem*).

generation intelligent satellites increased the resolution of remote sensing satellite data in the spatial, spectral and time dimension (Zhang, Wu, Zhao, Chanussot, Hong, Yao, and Gao 2023, 1814). At the same time, the satellite image quality and precision⁵³ has strongly increased, along with the speed of real-time analysis.

Given this background, policy makers should take into account concerns associated with the use of AI systems, in general. More precisely, space scientists and policy makers must consider that the multifaceted nature of AI has caused great controversy and confusion among scholars – e.g., in the fields of computer science, philosophy, mathematics – regarding the technology’s clear nature, definition and scope. Thus, the prevailing view is that AI may be divided into four broad categories, based on the fundamental differentiation between systems able to think or act like humans, from those able to think or act rationally (Kok, Boers, Kusters, and Van der Putten 2009, 1-5; Hassani, Silva, Unger, TajMazinani, and Mac Feely 2020, 146-147)⁵⁴. However, a more practical approach suggests distinguishing AI systems taking only into account the algorithms being used, in light of their capacity to replace the human brain; in this case, AI devices are divided into three broad categories, that is, Narrow Intelligence, Human level Artificial Intelligence and Super-intelligence (Fourtane, 2019).

Hence, according to the latter approach, the first category (i.e., Narrow Intelligence) is the one including most AI systems today, as these are mainly devices able to directly provide us with the solution of a specific problem, such as when they are programmed to recognize the biometric data of an individual, or his/her face. In theory, using this category of smart devices – which are significantly different from conventional computer programs, given their ability to learn – can bring major benefits for the national security

⁵³ Von der Dunk (2013, 243-244) argues that the resolution of very high resolution (VHR) data freely available on the commercial markets has recently dipped below the 0,5 m mark, and continues to evolve “downwards”.

⁵⁴ For the Turing approach to “intelligent”, proposed in 1950; see analytically Ertel (2017, 4).

policy, and allow to face, in a timely fashion, threats against States and citizens (e.g., terrorism). For comparison purposes, it may be noted that the second category (i.e., Human level Artificial Intelligence) refers to devices with human-like intelligence capabilities, such as those able to understand different languages in oral communication, promote a dialogue and develop specific thoughts; however, the greatest interest is currently focused on devices of the third category (i.e., Super-intelligence) which are still under development (according to scientists, Super-intelligence will be able to significantly exceed human mental abilities, discover new scientific methods and create new products and ideas). Therefore, up until now, it is Narrow Intelligence which is mainly being used in the context of space activity and exploration as well, as it is shown by SpaceX using (narrow) AI to find patterns in satellites, planets and space debris in order to keep their satellites safe in space (Lian 2022).

It is undisputable that AI used in RS will allow to strongly optimize information-gathering space technology, and that such a trend will be even more pronounced in the future. Nonetheless, it also appears that the combined use of RS technologies and AI data gathering techniques may infringe on specific privacy rights, such as information privacy and location privacy: more precisely, the first one “rests on the premise that information about ourselves is something over which individuals may exercise autonomy” (Maniadaki, Papathanasopoulos, Mitrou, and Maria 2021, 3), while the second one refers to “the right of individuals to move in their "home" and other public or semi-public places without being identified, tracked or monitored” (*ibidem*). In particular, the concern that the use of AI data processing combined with satellite imaging and VHR may pose threats to individual privacy is based on the fact that such tools can allow for large-scale facial recognition-based identification and unprecedented public surveillance, whether by a governmental or by private entities (Gal, Santos, Rapp, Markovich, and Van der Torre 2020, 14-17).

From this particular angle, it is feared that the uncontrolled use of AI devices could – intentionally or unintentionally – cause significant risks to the safety of citizens and States, such as by putting in danger persons’ privacy or even the public interest, independently of the sector in which they are being exploited.⁵⁵ Put differently, the challenge is now to find a way forward which will strike a balance between on the one hand technological development and high-resolution massive data gathering (which remains the clear direction to follow, in the context of globalization), and individual’s legal and ethical rights to privacy (Coffer 2020, 6453-6454) on the other hand.

4. Globalization, (AI) Data Gathering, Privacy Protection: Potential Solutions

Undoubtedly, activities pertaining to massive (AI) data gathering are enhanced by the accelerating pace of globalization and facilitated⁵⁶ by the use of space technology. Indeed, cross-border data flows are the hallmarks of the 21st century globalization⁵⁷ as, according to IDC, the Global Datasphere will grow from 33 zettabytes in 2018 to 175 zettabytes by 2025 (Reinsel, Gantz, and Rydning 2018, 3). Literally, massive data gathering is both a result of globalization, and a necessary tool for the improvement of technology – which is, as initially mentioned, at the heart of the globalization process –, such as deep learning applications and data-centric AI (Whang, Roh, Song, and Lee 2023, 794-795).

In this context, AI, machine learning methods and algorithms used in satellites seem to provide a promising solution which, however, raises a

⁵⁵ What is artificial intelligence and how is it used?, in *European Parliament website* (2020), <https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used>.

⁵⁶For example, some authors support that: “a new wave of commercial satellites imaging companies is collecting upwards of 100 terabytes of data per day” (Monhey 2020). Meanwhile, NASA’s Earth science data archive was around 40 petabytes in 2021 and is expected to hold more than 245 of data by 2025. More info available on <https://www.jpl.nasa.gov/news/nasa-turns-to-the-cloud-for-help-with-next-generation-earth-missions>.

⁵⁷Cp. supra note 5.

number of concerns. Effectively, as analyzed above, the application of data protection laws and regulations for data gathering and processing through AI in outer space remains a challenge, given that the use of AI in space allows to escape the limitations of territoriality. At the same time, such regulation seems to be necessary, due to the potential risks posed by AI technology, especially taking into account the fact that data gathering through the use of advanced-technology satellites is not any more a state's monopoly (and is therefore beyond the strict control of States⁵⁸).

By way of illustration, two of the most significant private satellite companies are Digital Globe and Spot Image; these commercial entities use their remote sensing satellites to gather various sorts of data – i.e., images, location data and real-time surveillance data – and then sell that satellite data to both the private sector and governments (Mckenna, Gaudion, and Evans 2019,612). Along with that, it is clear that all kinds of small satellites shall be increasingly used in the next years for EO and communication (Larsen 2017, 276-279), and that such development will facilitate an even greater involvement of private space actors.

Therefore, against the background of an increasing interdependence between globalization – requiring globalized markets and communication – and the massive collection and processing of data, as currently encouraged by cutting-edge space technologies, the question arises as to whether limits should be set for the conduct of such activity and, in case, what kind of limits.

As regards the first question, it is beyond doubt that the protection of personal data and privacy in the context of new technologies has become a key priority for most countries. Hence, the most probable scenario is that governments shall be challenged to ensure that their policies and legislation will ensure a minimum level of protection of personal data, even when these

⁵⁸ Private entities gather huge volumes of personal data and data breaches affecting millions of users are far too common. For example, a data breach from Yahoo in 2013 had an impact on 3 billion accounts and two recent data breaches from LinkedIn and Facebook (in 2021 and 2019) had an impact on 700 million and 533 million users (Hill and Swinhoe 2022).

are collected via space technology. However, the framework in which this protection may be achieved remains to be defined.

As a response, a few approaches (i.e., in reference to the second question) could be discussed; in particular, these could be classified into two categories: (4.1) application of existing legal tools to massive (AI) data gathering from space, and (4.2) adoption of a new legal instrument, taking into account the particular nature and the dynamics of said activity.

4.1 Use of Existing Instruments to Regulate (AI) Data Gathering from Space

As mentioned above, one of the key features of the regime applying to space activities is the freedom to use and exploit space for peaceful reasons, established as a principle first in the U.N. General Assembly Resolution 1721 (XVI) adopted in 1961,⁵⁹ and reiterated in the OST. Namely, Art. 1 (b) of the Resolution clearly noted that: “Outer space and celestial bodies *are free for exploration and use* by all states in conformity with international law ...”. On this basis, any massive (AI) space data gathering activities are *ab initio* lawfully conducted under international space law, provided they are carried out for peaceful purposes.

Seen from this angle, it additionally appears that massive (AI) data gathering is not precisely addressed by Resolution 1721, the OST or by international space law in general, leaving individuals unprotected from potential risks or harms that could result from this activity. In truth, the OST, its follow-on treaties developed through COPUOS and Res. 41/65 on the Principles on Remote Sensing Activity, do not provide any direct or indirect limitation to the generation and distribution of satellite data (including VHR) specifically addressing possible concerns of individuals or companies’ privacy (Von der Dunk 2013, 243-244). However, some kind of protection could still be granted based on some general provision of the OST; therefore, a first solution would be to ensure the legal protection of individuals’ privacy by applying to AI data collection in outer space some specific rules of the

⁵⁹ RES 1721 (XVI), International Co-operation in the Peaceful Uses of Outer Space.

OST. This option could be grounded on two different approaches and legal bases, as developed below.

4.1.1 Application of National Laws on the Basis of Art. VIII of the OST

According to Art. VIII of the OST, each State of Registry shall retain “jurisdiction and control” over their space objects and “over any personnel thereof, while in outer space or on a celestial body”.⁶⁰ On this basis, limits established in the national laws of the State of Registry could be imposed on massive (AI) data gathering carried out onboard space objects. In other words, States will be able to apply *mutatis mutandis* the same limits as the ones that were initially adopted in their domestic laws to regulate massive (AI) data gathering activities conducted in or *via* outer space; still, said national rules will apply in space only provided a State qualifies as the State of Registry.

Notwithstanding, in this case, all the weaknesses in the national laws will be – by the same token – transposed in the new context. To just take one example, there is no consensus in the legal literature on a definition of the right to privacy.⁶¹ According to some experts, privacy should be considered as “the right to be le(f)t alone” (Warren and Brandeis 1890, 193-195), whereas others define said concept as “the control over when and by whom the various parts of us can be sensed by others” (Parker 1974, 281). Thus, divergences from one legal system to another in the interpretation of concepts and terms may be detrimental to homogeneity and legal certainty, while entailing a risk for forum-shopping (in this case, “State of Registry-shopping”). Contrary to that, international space law aims at establishing uniformity to enable the conduct of space activity, to guarantee the protection of fundamental values and to encourage collaboration between States and

⁶⁰ States of Registry are defined in line with Art. I (c) of the Registration Convention, as “a launching State on whose registry a space object is carried in accordance with article II”; Art. II para. 1 of the Registration Convention clarifies that “the launching State shall register the space object”.

⁶¹ Art. 12, Universal Declaration of Human Rights, Paris, UN GA Res. 217 A (III) of 10 December 1948. A/RES/217; Art. 17 International Covenant on Civil and Political Rights, New York, done 19 December 1966, entered into force 23 March 1976.

actors. As a result, applying national protective measures on the basis of Art. VIII of the OST would not only undermine said goal of uniformity but the core spirit of international space law, especially considering the uncertainty caused by divergences in the interpretation of legal concepts.

As an alternative, a broad interpretation of the initial OST provisions (that is Art. I and III) could be used to introduce the idea that all space activities must be conducted in accordance with international law, including the protection of privacy and personal data.

4.1.2 Broad Interpretation of OST Articles: Applicability of International Law

On the basis of the OST, Art. I⁶² and Art. III,⁶³ all space activities must be carried out in accordance with international law *lato sensu*; the obligation applies to both governmental and non-governmental entities (i.e., it applies directly to States and State operators, as they are bound by international law; and indirectly to non-State operators, given that Art. VI of the OST stipulates that all kinds of space activities are imputed to States and involve direct State responsibility)⁶⁴. However, neither the OST nor the other treaties of international (space) law may literally be used for the purpose of data protection; in truth, said instruments were drafted long before the time of data and data markets, and they did not even begin to address the challenge of the commercial use of outer space for *inter alia* data gathering and/or data processing (Zoltick and Colgate 2019, 9-10). Hence, the question arises of whether data protection rules could be regarded as part of international law,

⁶² OST, Art. I para. 2: “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”.

⁶³ OST, Art. III: “States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law”.

⁶⁴ States usually ensure that private space operators abide by international space law treaties, so as not to be held responsible for any internationally wrongful act of said operators.

and be in an indirect way binding upon entities which are collecting data from outer space pursuant to the OST, Art. I and III, and/or Art. VI.

In response, it must first be highlighted that – despite its importance – there is not yet any international legal instrument to address the issue of private data protection. Nonetheless, as mentioned above, regional data privacy laws were adopted and are applicable within specific boundaries, such as the EU General Data Protection Regulation (GDPR)⁶⁵. Interestingly, data protection laws usually include specific provisions allowing to apply the rules that they adopt to non-residents on the basis of extraterritorial applicability provisions. By way of illustration, Art. 3 of Brazil’s LGPD states that: “This Law applies to any processing operation carried out by a natural person or a legal entity of either public or private law, irrespective of the means, the country in which its headquarter is located or the country where the data are located, provided that: (i) the processing operation is carried out in the national territory; (ii) the processing activity is aimed at the offering or provision of goods or services, or at the processing of data of individuals located on the national territory; or (iii) the personal data being processed were collected in the national territory. Similarly, Art. 3 (2) of the GPDR reads that ‘this regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union’.⁶⁶ Hence, Art. 3(2) increases the scope of EU data protection rules in a unilateral way, “and to a greater extent than any other

⁶⁵ Furthermore, following enforcement of the GDPR, some other countries adopted similar laws, such as Brazil (General Data Protection Law – LGPD), South Africa (Protection of Personal Information - POPIA) and Canada (Personal Information Protection and Electronic Documents Act – PIPEDA). More info available on: <https://securiti.ai/data-privacy-laws>.

⁶⁶ According to Recital 24 of the GDPR: “The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behavior of such data subjects in so far as their behavior takes place within the Union”.

jurisdiction in the world has done until now” (Azzi 2018, 130). Be that as it may, this is far from being rules of international law that could apply to space activity on the basis of the OST provisions mentioned above.

Alternatively, the obligation to take into account the protection of individuals’ privacy while conducting data gathering within the context of space activity could be inferred from Art. VII of the OST; said provision stipulates that “Each State Party (...) that launches or procures the launching of an object (...) is internationally liable for *damage* to another State Party (...) or to its natural or juridical persons by such object (...) on the Earth, in air space or in outer space”.⁶⁷ Hence, a country could be held liable to another one, in case an object launched from the first country resulted in a data breach of “juridical persons” of the second one; still, States (and space operators) should only be responsible in the event that the data breach occurs by launching an object into space (Zoltick and Colgate 2019, 8). From a practical perspective, such a situation is for the time being more or less unlikely.⁶⁸

In addition to that, a major downside of approaches based on a broad interpretation of specific OST or other treaties articles, is that they lack efficient enforcement mechanisms (Isnardi 2020, 512-515). Effectively, international space law does not provide a dispute resolution body, apart from the Liability Convention (1972) and the Registration Convention (1976) creating enforcement authorities with a very specific competence.

By way of illustration, the Liability Convention established in Art. IX to Art. XX a dispute settlement system comprising both a diplomatic⁶⁹ and an

⁶⁷ Emphasis added.

⁶⁸ “The proliferation of emerging digital technologies is expected to render more relevant/significant in the future types of material or non-material damage (e.g., economic losses or damage to or destruction of data that could be considered a property loss) which are considered currently as falling outside the restrictive scope of recoverable damage under the Liability Convention” (Kyriakopoulos, Pazartzis, Koskina, and Bourcha, 2021).

⁶⁹ Liability Convention of 1972, Art. IX: “A claim for compensation for damage shall be presented to a launching State through diplomatic channels. If a State does not maintain diplomatic relations with the launching State concerned, it may request another State to present its claim”.

arbitration⁷⁰ phase, before a Claims Commission; this mechanism has been tested once in the Cosmos 954 incident (Beck 2009, 15). However, as no enforcement procedure was established by the Liability Convention – i.e., the Claims Commission only has a quasi-judicial power;⁷¹ according to Art. XIX (2)⁷² its decisions shall be final and binding only if the parties have agreed so⁷³ – the implementation of its decisions depends to a large extent on political pressure and criticism. On this basis, said mechanism was regarded to be ineffective and widely criticized (Gomez 2012); it may therefore not be considered to be a viable judicial system that could be furthermore applied to novel issues.

Overall, there is no doubt that approaches based on the possible application of existing instruments are both interesting and defensible, but they also have a significant weakness which lies in the fact that all treaties of international space law were adopted for a general purpose and they do not seem to be well adapted to regulate massive (AI) data collection from space, for all the reasons explained above. At the same time, there are concerns that the use of AI may be problematic (e.g., abusive) *per se*, due to the opaque nature of the systems leading to an inability for an individual to understand how the results of AI processes came about, also referred to as the black box AI problem (Blasch, Sung, Nguyen, Daniel, and Mason 2019, 2).

Hence, as the reliance on AI systems is regarded as inherently risky – which is illustrated by the fact that States have already regulated many of its uses – a different possible approach would be to take into account that AI is

⁷⁰ Liability Convention of 1972, Art. XIV: “If no settlement of a claim is arrived at through diplomatic negotiations as provided for in Article IX, within one year (...), the parties concerned shall establish a Claims Commission at the request of either party”.

⁷¹ Namely, the Claims Commission’s does not have the same authority as a judicial court (Isnardi 2020, 513-514).

⁷² Liability Convention of 1972, Art. XIX (2): “The decision of the Commission shall be final and binding if the parties have so agreed; otherwise, the Commission shall render a final and recommendatory award, which the parties shall consider in good faith”.

⁷³ Hence, this alternative dispute resolution method cannot be considered as “genuine arbitration” since the binding effect of the award depends on the common will of the parties. One of the fundamental distinctive features of an arbitration award is that is binding to the parties, so they are not at liberty to accept or reject it (Ikeyi and Maduka 2014, 328).

a topic that really needs specific attention. Thus, it may be argued that a coordinated and unified approach is required, able to potentially result in the adoption of a new instrument regulating massive (AI) data collection precisely in case such activity is carried out in/from space.

4.2 A New Instrument that Would be Applicable to Data Gathering From Space

It is only logical to argue that the scientific developments in the field of AI should give fresh impetus to international negotiations, aimed at the development of more specific and well-adapted rules of international law applying precisely to massive (AI) data gathering from space. In particular, States could agree to adopt a new agreement, to regulate the scope and limitations of such activity while insisting on proper protection against abusive collection and processing of private data. Such agreement could be finalized in a treaty, perhaps similar to the Nuclear Test Ban Treaty⁷⁴ prohibiting the conduct of nuclear explosions in space.

The rationale for adopting a specific treaty would be that most legal instruments in place do not address the topic of private data protection, in case such activity is conducted in or via outer space. By way of illustration, Chapter 5 of the GPDR entitled “[t]ransfers of personal data to third countries or international organizations” remains silent with respect to transfers of data outside of the Earth (Zoltick and Colgate 2019, 9); as a result, neither public nor private space operators may be subject to the GPDR mandatory provisions in case of transfers of personal data to or via outer space. Put differently, a new regulatory scheme seems to be required to fill this type of gap (*ibidem*).

Such a solution would entail uniformity and legal certainty, however under the condition that States would effectively ratify it. In truth, “no additional

⁷⁴ Treaty banning nuclear weapon tests in the atmosphere, in outer space and under water (Partial Test Ban Treaty - PTBT), 5 August 1963, UNTS 480 (43) (EIF 10 October 1963), Art. I.

treaties have been concluded – through the UNCOPUOS or other similar fora – in international space law, since the Moon Agreement was adopted in 1979; in a world where competition for space matters is growing, soft law guidelines and codes of conduct have proven more adequate”.⁷⁵ Be that as it may, taking into account the wide-scale adoption of the Paris Agreement signed in 2015, whereby all member States committed to taking action on climate change due to the growing public awareness of this issue, the possibility of adopting a treaty reflecting an international consensus on the acceptable uses of AI in the context of space data gathering, and abiding by it, should not be *a priori* excluded. Otherwise, a non-binding instrument (namely, based on a bottom-up initiative) comparable to the guidelines on space debris mitigation could be considered (Stokes, Akahoshi, Bonnal, Destefanis, Gu, Kato, Kutomanov, LaCroix, Lemmens, Lohvynenko, Oltrogge, Omaly, Opiela, Quan, Sato, Sorge, and Tang 2020, 326-328); indeed, the guidelines – first adopted by space operators within the IADC⁷⁶ – are now largely applied and endorsed by the ITU (Perek 2004, 223-224), due to their efficiency and practical feasibility.

In essence, the principal issue to address would be the fact that collecting sensitive data by AI in/via outer space does not – technically – require any consent from the subject concerned. From this perspective, some scholars argue that massive (AI) data collection based on the use of high-resolution satellite imagery could pave the way for mass surveillance and result in the abolition of autonomy in the new digital world (Franckiewicz 2023). Thus, “resolving these many challenging legal questions will require creative and flexible solutions as soon as possible (Jasentuliyana 2001, 21)”.⁷⁷

Taking these points into account, a new regulatory framework should build upon the existing principles enshrined in data protection laws, to ensure that

⁷⁵ There has been a strong tendency towards the development of soft law guidelines and “codes of conduct” for space-related matters, notwithstanding the inherent risks that this (potentially) brings of greater “on-compliance” (Jakhu and Freeland 2016).

⁷⁶ Inter-Agency Space Debris Coordination Committee (IADC). IADC space debris mitigation guidelines, IADC-02-01, Revision 2, March 2020.

⁷⁷ In the same vein, see also Koskina and Angelopoulou (2022, 39).

any development and use of AI is compatible with the protection and fulfillment of fundamental human capacities and goals (Montreal Declaration, 2018: see Soroka and Kurkova 2019, 137); alternatively, AI systems must be used in line with the laws ensuring the effective application of fundamental rights, such as the rights to privacy and data protection (e.g., EU principles of proportionality). This, in conjunction with the fact that fundamental protective principles – e.g., the classification rules for high-risk AI systems as proposed by the European Commission⁷⁸ and the fairness and transparency (Walmsley 2021, 586-589) of AI data processing applications – should be recognized, and priority given to an effective (that is, human) control of AI and AI uses. Indeed, pursuant to Art. 14 of the Commission’s proposal, “high-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use”. In line with this, it is noteworthy that the new Greek legal framework on emerging information and communication technologies⁷⁹ establishes the obligation of public authorities to disclose information about the commencement of operation and the operating parameters of the AI system as well as on the decisions taken through AI.⁸⁰

In any case, the establishment of a law enforcement mechanism (of a quasi-judicial nature, or even based on arbitration) would be necessary under a new international treaty in order to ensure the protection of public and private rights via final and binding awards. Overall, the final aim should be to ensure the use of outer space in a manner that would be respectful of both stakeholders’ interests and fundamental human rights.

⁷⁸ COM/2021/206, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>.

⁷⁹ Greek Law n° 4961/2022 “on emerging information and communication technologies, the reinforcing of digital governance and other provisions” (GG 146/A/27-07-2022).

⁸⁰ Art. 6 of Greek Law n° 4961/2022.

5. Conclusive Remarks

As the foregoing analysis suggests, the extensive use of artificial intelligence techniques in the context of data gathering and processing in/from space may be regarded as one of the greatest challenges facing humanity today. Hence, there is an urgent need to strike a balance between the development of (AI) data collection technology and the protection of the fundamental rights of both individuals and States, especially given the fact that technologies – such as AI – and innovation are the most dynamic force behind globalization.

In the era of digital globalization, cross-border data flows coupled with the distribution of personal data derivatives create more and more complex issues. On this basis, the first step would be to strengthen transnational cooperation under the auspices of the United Nations in order to foster the adoption of commonly accepted principles for AI data gathering in space; special attention should be given to the role of developing countries with the aim to gradually reduce the technological gap between them and the developed economies. Still, a second step should be the adoption of a new international agreement with well adapted provisions, coupled with an efficient dispute resolution mechanism eventually building upon existing data protection laws (e.g., the GPDR may be a useful tool for the development of such a framework).

Be that as it may, basic concepts like the ‘informed consent’ by individuals and, the principle of proportionality and transparency in the use of artificial intelligence must be the basis of such a new framework. Nevertheless, in the event that including such rules as those ensuring the data subject’s consent or AI transparency proves impossible in case of massive (AI) data gathering conducted in/from space, the suggested framework should incorporate human control over said the way AI systems are used in order to provide a minimum level of protection.

References

- Abney K. (2020). Space war and AI, in Y. Masakowski (ed.), *Artificial Intelligence and Global Security* (Emerald).
- Azzi A. (2018). The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, n. 9.
- Baker C. (2003). Tolerance of International Espionage: A Functional Approach, in *American University International Law Review*, n. 19.
- Beck B. (2009). The Next, Small, Step for Mankind: Fixing the inadequacies of the International Space Law treaty regime to accommodate the modern space flight industry, in *Journal of Science and Technology*, n.19.
- Blasch E., Sung J., Nguyen T., Daniel C., and Mason A. (2019). Artificial Intelligence Strategies for National Security and Safety Standards, *ArXiv*, <https://arxiv.org/abs/1911.05727>.
- Bohlmann U., and Soucek A. (2018). From “Shutter Control” to “Big Data”: Trends in the Legal Treatment of Earth Observation Data, in C. Brünner, G. Königsberger, H. Mayer, and A. Rinner (eds.), *Satellite-Based Earth Observation* (Springer).
- Boldirini E., Nativi S., Hradec J., Santoro M., Mazzetti P., and Craglia M. (2023). GEOSS Platform data content and use, in *International Journal of Digital Earth*, n. 16.
- Breen S., Ouazzane K., and Patel P. (2020). GDPR: Is your consent valid? in *Business Information Review*, n. 37.
- Butterworth M. (2018). The ICO and artificial intelligence: the role of fairness in the GDPR framework, in *Computer Law & Security Review: The International Journal of Technology Law and Practice*, n. 34.
- Butterworth R. L. (2012). *Space and the Joint Fight* (Strategic Forum National Defense University Press).
- Coffer M. (2020). Balancing Privacy Rights and the Production of High-Quality Satellite Imaginary, in *Environmental Science & Technology*, n. 54.

Copeland M., Soh J., Puca A., Manning M., and Gollob D. (2015). *Microsoft Azure Planning, Deploying, and Managing your Data Center in the Cloud* (Apress).

Doldirina C. (2015). Open Data and Earth Observations: The Case of Opening up Access to and Use of Earth Observation Data Through the Global Earth Observation System of Systems, in *Journal of Intellectual Property, Information Technology and E- Commerce Law*, n. 6.

Ertel W. (2017). *Introduction to Artificial Intelligence* (2nd ed.) (Springer).

Fourtane S. (2019). The Three Types of Artificial Intelligence: Understanding AI, *Interesting Engineering*,
<https://interestingengineering.com/innovation/the-three-types-of-artificial-intelligence-understanding-ai>.

Franckiewicz M. (2023). Satellite Surveillance: A Balancing Act Between Security and Privacy, *TS2 Space*, <https://ts2.space/en/satellite-surveillance-a-balancing-act-between-security-and-privacy>.

Fu W., Ma J., Dei C., Fang C. (2020). Remote sensing Satellites for Digital Earth, in H. Guo, M.F. Goodchild, and A. Annoni (eds.), *Manual of Digital Earth* (Springer).

Gabriel I. (2020). Artificial Intelligent, Values and Alignment, in *Minds and Machines*, n. 30.

Gal G., Santos C., Rapp L., Markovich R., and Van der Torre L. (2020). Artificial Intelligence in Space, *arXiv*, <https://arxiv.org/abs/2006.12362>.

Gevaert C. (2022). Explainable AI for earth observation: A Review including societal and regulatory perspectives, in *International Journal of Applied Earth Observations and Geoinformation*, n. 112.

Gharbi R.B., and Mansoori G.A. (2005). An introduction to artificial intelligence applications in petroleum exploration and production, in *Journal of Petroleum Science and Engineering*, n. 49.

Gomes V., Queiroz G., and Ferreira K. (2020). An Overview of Platforms for Big Earth Observation Data Management and Analysis, in *Remote Sensing*, n. 12:1253.

Gomez C. (2012). The Optional Rules of Arbitration of Disputes Relating to Outer Space Activities of the Permanent Court of Arbitration, a Real Option for the Solution of Conflicts in Space Matter? in *Proceedings of the International Astronautical Congress, 2012*: <https://ssrn.com/abstract=2963687>.

Goodman B. and Flaxman S. (2017). European Union regulations on algorithmic decision-making and a “right to explanation”, in *AI Magazine*, n. 38.

Guerrisi G., Del Frate F., and Schiavon G. (2022). Satellite On-Board Change Detection via Auto-Associative Neutral Networks, in *Remote Sensing*, n.14.

Hanson C. W., and Marshall B.E. (2001). Artificial intelligence applications in the intensive care unit, in *Critical Care Medicine*, n.29.

Hashemipour S., and Maaruf A. (2020). Amazon Web Services (AWS) – An Overview of the On-Demand Cloud Computing Platform, in M. Miraz, P. Excel, A. Ware, S. Soomro, and M. Ali (eds.) *Emerging Technologies in Computing* (Springer).

Hassani H., Silva E., Unger S., TajMazinani M., and Mac Feely S. (2020). Artificial Intelligence (AI) or Intelligence Augmentation (IA): What Is the Future, in *AI*, n.1.

Hill M., and Swinhoe D. (2022). The 15 biggest data breaches of the 21st century, *CSO Online*, <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.

Horowitz M.C., Allen G.C., Kania E.B., and Scharre P. (2018). Strategic Competition in an Era of Artificial Intelligence, in *Artificial Intelligence and International Security series (CNAS)*, http://www.indexfunds.org/resources/Research-Materials/NatSec/-Strategic_Competition_in_Era_of_AI.pdf.

Huffer B., Cotnoir M., and Gleason J. (2015). Ontology-drive data access at the NASA earth exchange, in *2015 IEEE International Conference on Big Data, Santa Clara, CA, USA*.

- Humerick M. (2018). Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, in *Santa Clara High Technology Law Journal*, n. 34.
- Ikeyi N., and Maduka T. (2014). The Binding Effect of a Customary Arbitration Award: Exorcizing the Ghost of *Agu v Ikewibe*, in *Journal of African Law*, n. 58.
- Ishii K. (2019). Comparative legal study on privacy and general data protection for robots equipped with artificial intelligence: looking at functional and technological aspects, in *AI and Society*, n. 34.
- Islam M.S. (2018). The Sustainable Use of Outer Space: Complications and Legal Challenges to the Peaceful Uses and Benefit of Humankind, in *Beijing Law Review*, n. 9.
- Isnardi C. (2020). Problems with Enforcing International Space Law on Private Actors, in *Columbia Journal of Transnational Law*, n. 58.
- Iyer L.S. (2021). AI enabled applications towards intelligent transportation, in *Transportation Engineering*, n. 5.
- Jakhu R., and Freeland S. (2016). The relationship between the Outer Space Treaty and customary International Law, in *Proceedings of the 67th International Astronautical Congress* ,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3397145.
- Jasentuliyana N. (2001). International Space Law Challenges in the Twenty-first Century, in *Singapore Journal of International and Comparative Law*, n. 5.
- Joyner C. (1999). The United Nations and Democracy, in *Global Governance*, n. 5.
- Kakani V., Nguyen V.H., Kumar B.P., Kim H., and Pasupuleti V.R. (2020). A critical review on computer vision and artificial intelligence in food industry, in *Journal of Agriculture and Food Research*, n. 2.
- Killough B. (2018). Overview of the Open Data Cube Initiative, in *IGARSS 2018 – IEEE International Geoscience and Remote Sensing Symposium, Valencia, Spain*.

- Klosowski T. (2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters), *Wirecutter* ,
<https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>
- Kok J., Boers E.J., Kusters W., and Van der Putten P, (2009). Artificial Intelligence: Definition, Trends, Techniques and Cases, in *Encyclopedia of Life Support Systems*, vol. I (UNESCO).
- Koskina A., and Angelopoulou K. (2022). Space Sustainability in the Context of Global Space Governance, in *Athena – Critical Inquiries in Law, Philosophy and Globalization*, n. 2.
- Kumar S., Arivazhagan S., and Rangarajan N. (2013). Remote Sensing and GIS Applications in Environmental Sciences – A Review, in *Journal of Environmental and Nanotechnology*, n. 2.
- Kussul N., Shelestov A., Basarab R., Shakun S., Kussul O., and Lavreniuk M. (2015). Geospatial Intelligence and data fusion techniques for sustainable development problems, in *2015 International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications*.
- Kyriakopoulos G., Pazartzis P., Koskina A., and Bourcha C. (2021). Artificial Intelligence and Space Situational Awareness: data processing and sharing in debris-crowded areas, in T. Flohrer, S. Lemmens, and F. Schmitz (eds.), *Proc. 8th European Conference on Space Debris (virtual), Darmstadt, Germany, 20–23 April 2021* ,
<https://conference.sdo.esoc.esa.int/proceedings/sdc8/paper/118>
- Larsen P. (2017). Small Satellite Legal Issues, in *Journal of Air Law and Commerce*, n. 82.
- Latonero M. (2018). Governing Artificial Intelligence: Upholding human rights and dignity, *Data & Society*, <https://datasociety.net/library/governing-artificial-intelligence>.
- Lian R. (2022). How SpaceX uses AI?, *Community AI*,
<https://www.thecommunityai.org/ai-blog/ai-on-spacex>.

- Maldoff G. (2016). Top 10 Operational Impacts of the GDPR: Part 3 – Consent, *IAPP*, <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent>.
- Maniadaki M., Papathanasopoulos A., Mitrou L., Maria E.-A. (2021). Reconciling Remote Sensing Technologies with Personal Data and Privacy Protection in the European Union: Recent Developments in Greek Legislation and Application Perspectives in Environmental Law, in *LAWS*, n. 10.
- Marin L. (2016). The fate of the Data Retention Directive: about mass surveillance and fundamental rights in the EU legal order, in V. Mitsilegas, M. Bergström, and T. Konstadinides (eds.), *Research Handbook on EU Criminal Law* (Elgar).
- Martin A., and Freeland S. (2021). Back to the Moon and Beyond: Strengthening the Legal Framework for Protection of the Space Environment, in *Air and Space Law*, n. 46.
- Martin S.A., and Freeland S. (2021). The Advent of Artificial Intelligence in Space Activities: New Legal Challenges, in *Space Policy*, n. 55.
- Martinez R. (2019). Artificial Intelligence: Distinguishing Between types and definitions, in *Nevada Law Journal*, n. 19.
- Mattoo A., and Meltzer J.P. (2018). International Data Flows and Privacy: The Conflict and Its Resolution, in *Journal of International Economic Law*, n. 21.
- Mckenna A., Gaudion A, and Evans J. (2019). The Role of Satellites and Smart Devices: Data Surprises and Security, Privacy, and Regulatory Challenges, in *Penn State Law Review*, n. 123.
- Milaj J. (2016). Privacy, surveillance, and the proportionality principle, in *International Review of Law, Computers and Technology*, n. 30.
- Mitrou L. (2018). Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof?’, *SSRN Electronic Journal*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914.
- Monhey D. (2020). Terabytes from Space: Satellite Imaging is Filling Data Centers, *Data*

Center Frontier, <https://www.datacenterfrontier.com/internet-of-things/article/11429032/terabytes-from-space-satellite-imaging-is-filling-data-centers>.

Navarrete I., and Buchan R. (2019). Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions, in *Cornell International Law Journal*, n. 51.

Nayak B., and Walton N. (2023). The future of platforms, big data and new forms of capital accumulation, *Information Technology and People*, <https://doi.org/10.1108/ITP-05-2022-0409>.

Nicholas M. (2019). Espionage, in *The Histories*, n. 5.

Parker R. (1974). A definition of privacy, in *Rutgers Law Review*, n.27.

Perek L. (2004). Space Debris Mitigation and Prevention: How to Build a Stronger International Regime, in *Astropolitics*, n. 2.

Politou E., Alepis E., and Patsakis C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions, in *Journal of Cybersecurity*, n. 4.

Reinsel D., Gantz J., and Rydning J. (2018). The Digitization of the World from Edge to Core, *IDC*, <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>.

Scherer M. (2016). Regulating artificial intelligence systems: risks, challenges, competencies, and strategies, in *Harvard Journal of Law & Technology*, n. 29.

Sevalnev V.V., and Tsirin A.M. (2022). Globalization Using Network Effects, in M. Inozemtsev, E. Sidorenko, and Z. Khisamova (eds.), *The Platform Economy – Designing a Supranational Framework* (Palgrave Macmillan).

Sinha A. (2012). Remote Sensing Satellites: Legal Issues in Emerging Technology, in R. Singh, S. Kaul, and S. Rao (eds.) *Current Developments in Air and Space Law* (National University Law Press).

- Soroka L., and Kurkova K. (2019). Artificial Intelligence and Space Technologies: Legal, Ethical and Technological Issues, in *Advanced Space Law*, n. 3.
- Stefoudi D. (2017). Space big data: Big Data troubles in the final frontier, <https://www.leidenlawblog.nl/articles/space-big-data-big-data-troubles-in-the-final-frontier>.
- Stokes H., Akahoshi Y., Bonnal C., Destefanis R., Gu Y., Kato A., Kutomanov A., LaCroix A., Lemmens S., Lohvynenko A., Oltrogge D., Omaly P., Opiela J., Quan H., Sato K., Sorge M., and Tang M. (2019). Evolution of ISO's space debris mitigation standards, in *Journal of Space Safety Engineering*, n.7.
- Von der Dunk F.G. (2009). European Satellite Earth Observation: Law, Regulations, Policies, Projects and Programmes, in *Creighton Law Review*, n. 42.
- Von Der Dunk F.G. (2013). Outer Space Law Principles and Privacy, in D. Leung, and R. Purdy (eds.), *Evidence from Earth Observation Satellites: Emerging Legal Issues* (Brill).
- Walmsley J. (2021). Artificial intelligence and the value of transparency, in *AI & Society*, n. 36.
- Wang P. (2019). On Defining Artificial Intelligence, in *Journal of Artificial General Intelligence*, n. 10.
- Warren S., and Brandeis L. (1890). The right to privacy, in *Harvard Law Review*, n. 4.
- Wasilow S., and Thorpe J. B. (2019). Artificial Intelligence, Robotics, Ethics, and the Military: A Canadian Perspective, in *AI Magazine*, n. 40.
- Weiss M., Jacob F., and Duveiller G. (2020). Remote sensing for agricultural applications: A meta-review, in *Remote Sensing of Environment*, n. 236.
- Whang S., Roh Y., Song H., and Lee J.- G. (2023). Data collection and quality challenges in deep learning: a data-centric AI perspective, in *The VLDB Journal*, n. 32.

- Yashchenko V. (2014). Artificial Intelligence Theory (Basic concepts), in *Science and Information conference, London, August 2014*, <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6918230>.
- Zeller B., Trakman L., Walters R., and Rosadi S. (2019). The Right to be Forgotten-The EU and Asia Pacific Experience (Australia, Indonesia, Japan and Singapore), in *European Human Rights Law Review*, n. 1.
- Zhang B., Wu Y., Zhao B., Chanussot J., Hong D., Yao J., and Gao L. (2022). Progress and Challenges in Intelligent Remote Sensing Satellite Systems, in *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, n. 15.
- Zhao G., Yu L., Li X., Peng D., Zhang Y., and Gong P. (2021). Progress and Trends in the Application of Google Earth and Google Earth Engine, in *Remote Sensing*, n.18.
- Zhao Q., Yu L., Du Z., Peng D., Hao P., Zhang Y., and Gong P. (2022). An Overview of the Applications of Earth Observation Satellite Data: Impacts and Future Trends, in *Remote Sensing*, n. 14.
- Zoltick M., and Colgate J. (2019). The Application of Data Protection Laws in (Outer) Space, in *International Comparative Legal Guide to: Data Protection* (Global Legal Group).