Legal and policy aspects of space big data: legal implications of the use of large amounts of space data – regulatory solutions and policy recommendations

Stefoudi, D.

3 Legal aspects of the use of space big data

Relevant laws and data policies

This chapter focuses on research question 2, namely "what are current laws and data policies that are relevant to space big data based on their type and their uses?". To identify the relevant regulatory framework, the laws that apply to space data as a field of space activity and to space data as a source of information are taken into account. In particular, laws that relate to the collection, access to, use of, and dissemination of information collected, stored and transmitted by means of space technology are considered.

The legal aspects relevant to space big data consist of a patchwork of international and domestic space legislation, along with regional and national laws and data policies. In this thesis, emphasis is placed on EU law. EU regulations can be used as a reference for other national regulations thanks to their similarities, and some EU regulations have a wide scope of application. The laws of space-faring countries around the world are addressed as reference, where available. This chapter investigates the laws that apply to space big data and affect their collection, access, use, and dissemination. Space big data are collected, stored, and disseminated by means of space technology. Therefore, laws that govern the operation of satellites involved in the space big data lifecycle are addressed under international space law. Likewise, export regulations that impact space technology involved in the space big data lifecycle are also addressed. Considering that space big data contain and transmit information, information-related fields of law, such as privacy and data protection, intellectual property, and cybersecurity, are relevant. Space big data also include information that is governed by data policies focusing on the collection, access, use, and dissemination of space data.

This chapter examines the laws that are relevant to space big data, namely international space law (section 3.1), privacy and data protection law (section 3.2), intellectual property law (section 3.3), cybersecurity law (section 3.4), and export control law (section 3.5). It also investigates data policies that are applicable to space big data (section 3.6). Section 3.7 concludes the chapter and answers the second research question.

3.1 International space law

International space law comprises five international treaties and a set of UN Declarations and UN General Assembly Resolutions on various space matters,

along with legal documents of international organisations managing space activities.[1] Its purpose is to regulate the conduct of States and by extension of private entities, in outer space. Therefore, international space law constitutes the most relevant field of law concerning any type of space activity by way of its subject and scope. Except for its contextual proximity, international space law can be invoked as *lex specialis* of public international law, namely the specialised law that prevails over general laws in cases of conflict or doubt of applicable provisions.[2] Space big data and space big data applications are procured through space technology and are enabled by satellites that are launched into outer space, hence they fall under the scope of international space law.

This section identifies the parts of space law that are relevant to space big data and applications, in order to determine the extent to which they regulate current developments in the field of space big data, as well as the activities of the States and private actors involved therein. It also aims to provide background information and analysis of space law provisions that will appear in subsequent chapters. Section 3.1.1 elaborates on the general principles of the Outer Space Treaty[3] that are relevant to space big data. It is followed by provisions of the Outer Space Treaty, in conjunction with the Liability Convention[4] and the Registration Convention,[5] which concern the activities of private actors in outer space (section 3.1.2), the registration of space objects (section 3.1.3), and the liability for damage caused by space objects (section 3.1.4). Section 3.1.5 examines the harmful interference with space activities by reference to the provisions of the Outer Space Treaty, as well as to the instruments of the International Telecommunication Union (ITU). The latter are only consulted to describe the term 'harmful interference' as it appears in the Outer Space Treaty. Although other provisions of the space treaties may find application in specific cases, the ones addressed in section 3.1 have general application and relevance to space big data.

---

1 P Malanczuk, 'Space law as a branch of international law' (1994) 25 Netherlands Yearbook of International Law 143, 147; S Gorove, 'International space law in perspective - Some major issues, trends and alternatives' (1983) 181.3 Recueil de Cours 353, 357; N M Matte, 'Space policy: Today and tomorrow – The vanishing duopole' (1979) 4 Annals of Air and Space Law 567.

2 T Masson-Zwaan, M Hofmann, *Introduction to space law* (4th edn, Wolter Kluwers 2019), 5.

3 Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (opened for signature 27 January 1967, entered into force 10 October 1967) 610 UNTS 205 (hereinafter Outer Space Treaty, OST).

4 Convention on International Liability for Damage Caused by Space Objects (opened for signature 29 March 1972, entered into force 1 September 1972) 1023 UNTS 15 (hereinafter Liability Convention, LIAB).

5 Convention on Registration of Objects Launched into Outer Space (opened for signature 14 January 1975, entered into force 15 September 1976) 672 UNTS 119 (hereinafter Registration Convention, REG).

3.1.1 General provisions of the UN Space Treaties

The five international Space Treaties were negotiated and adopted by consensus by the UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS) with the purpose of regulating the activities of their member States in outer space. The Outer Space Treaty (OST) entered into force in 1967 and was the first international space law treaty to be adopted. It contains general principles regarding the space activities of States, which have been further developed in the articles of the subsequent four space treaties, namely the Rescue and Return Agreement of 1968 (ARRA),[6] the Liability Convention of 1972 (LIAB), the Registration Convention of 1975 (REG) and the Moon Agreement of 1979 (MA).[7] The Outer Space Treaty is the cardinal space law document and provides the fundamental guidelines that States must adhere to when conducting their activities in outer space.[8] It consists of principles that establish rights and obligations of general character, which, despite not addressing specific types of space conduct, find application in space activities procured by States and are often transferred into domestic legislations that govern the activities of private actors. They have also been consistently followed by agencies and organisations involved in space activities. In the scope of the space treaties and relevant to the present analysis, space activities refer to the launch and operation of satellites that collect, store, and transmit space data, as well as to any related activity that forms an integral part of these satellite systems. Provisions of particular relevance to space big data are the freedoms of outer space and the use of outer space for the benefit of humankind, enshrined in Article I OST, as well as the non-appropriation principle of Article II OST.

The Outer Space Treaty begins by laying down the essential principle of the freedom of exploration, use, and scientific investigation of outer space by all countries. This threefold freedom laid down in Article I OST, constitutes one of the main elements of international space law and sets the standard for the interpretation of other space law provisions.[9] As far as space big data are concerned, States are free to launch satellite systems that collect, store, and transmit space big data, and to conduct related activities, as long as the latter do not violate international law.[10] Space big data also fits the concept of

6 Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (opened for signature 22 April 1968, entered into force 3 December 1968) 672 UNTS 119 (hereinafter Rescue and Return Agreement, ARRA).

7 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (opened for signature 18 December 1979, entered into force 11 July 1984) 1363 UNTS 22 (hereinafter Moon Agreement, MA).

8 F Lyall, P B Larsen, *Space law: A treatise* (2nd edn, Routledge 2018) 50.

9 S Gorove, 'Freedom of exploration and use in the Outer Space Treaty: A textual analysis and interpretation' (1971) 1.1 Denver Journal of International Law and Policy 93, 101.

10 OST (n 3) art III.

Article I OST by facilitating and contributing to the use, exploration, and scientific investigation of outer space. Part of space big data comes from the observation of outer space from the Earth and Earth-based and space-based telescopes, hence space big data promotes scientific knowledge of both the terrestrial and extra-terrestrial environment. At the same time, space big data offered on an open access basis allow for these freedoms to be enjoyed by countries other than those that launched a satellite system or collected and processed the data. Likewise, commercial space data that are made available for purchase to any interested party fulfil this purpose.

Another fundamental space law principle laid out in Article I OST is that the conduct of space activities must be for the benefit and in the interest of all countries regardless of their economic, scientific, and other capabilities, and shall be the province of humankind.[11] Even though this principle does not mention any mechanisms through which benefit-sharing can be realised,[12] the knowledge and opportunities offered through space big data applications can constitute some of these methods. The use of space data for sustainability on the Earth and in outer space described in section 2.1.3 can serve as an example of the use of space activities for global benefit. The same applies to the connection of space big data applications with the principle of maintaining international peace and security and promoting international cooperation, as prescribed in Article III OST. Several applications, such as EO and space-based geolocation applications, are procured or deployed for purposes related to the identification of acts against peace or for monitoring areas under conflict.

Lastly in the scope of general provisions, Article II OST establishes that outer space is an area outside national sovereignty that cannot be appropriated by any State. Whereas the non-appropriation principle does not directly affect space big data, the fact that they are collected by satellites that operate in an

11 A discourse on the various meanings of the term 'mankind' can be found in M Lachs, *The law of outer space: An experience in contemporary law-making* (Sijthoff 1972) 23, 45 and 54; W Jenks, *Space law* (Stevens 1965) 194; E Fasan, 'The meaning of mankind in space legal language' (1974) 2 JSL 125, 130-131. The authors respectively support that humankind involves all countries or all peoples or the international community as a whole, that humankind refers to a general community, and that humankind could be considered as subject of international law. Cocca introduces the term res communis humanitatis to indicate a legal condition derived from the community of interests and benefits recognised in favour of humankind. A A Cocca, 'Determination of the meaning of the expression 'res communes humanitatis' in space law' in A G Haley (ed), *Proceedings of the sixth colloquium on the law of outer space* (IISL 1964) 1. The author of this thesis is of the view that the term 'mankind' should be replaced by 'humankind' in the space treaties and, when applicable, uses the term humankind.

12 In N Jasentuliyana, 'Article I of the Outer Space Treaty revisited' (1989) 17 JSL 129, 139-140 the author argues that it is not clear whether Article I imposes an obligation to share benefits and clarifies that no State had asserted, until then, any right to benefits obtained by another country on the basis of Article I OST. Some alternatives to consider to define benefits are presented in M Simpson, 'Benefit in space law: Principle and pathway' (2020) 45.2 ASL 143, 147-152.

area outside of national sovereignty may raise challenges when it comes to determining the laws applicable to them. This issue is further elaborated in chapter 4.

3.1.2 Activities of States and private actors in outer space

The space treaties are designed to regulate the activities of States in outer space but apply to the activities of private actors, which constitute a large part of the stakeholders involved in space big data, by means of Article VI OST.[13] However, Article VI OST provides that States are internationally responsible for the activities of their nationals in outer space and requires States to authorise and continuously supervise the space activities of their non-governmental entities.[14] Article VI OST thus extends the application of international space law to the activities of private entities. It also forms the basis for the establishment of national space legislation, for States to be able to regulate the conditions under which they are held accountable for the activities of their national natural and legal persons.[15]

In the field of space big data, the international responsibility of States is connected to the authorisation of private companies to perform activities related to space big data. Whereas few countries have specific regulations on space data, in most cases, such activities fall under the general licensing obligations for space activities. Space-faring countries provide licenses for the launch or operation of satellites and payloads, as well as for the operation of ground facilities.[16] These stages of a space activity may coincide with stages of the space big data lifecycle, namely the launch of satellites that generate or transmit space big data or the ground infrastructure where space big data are collected and processed. In this regard, space big data activities will be

13 F G von der Dunk, 'The origins of authorisation: Article VI of the Outer Space Treaty' in F G von der Dunk (ed), *National space legislation in Europe* (Studies in Space Law vol 6, Brill 2011) 9. More on the issue of private activities in outer space can be found in H A Wassenbergh, 'The unfreedom of outer space law' (1985) 10.3 ASL 161.

14 V S Vereshchetin, 'International space law and domestic law: Problems of interrelations' (1981) 9 JSL 31, 31 and 33. Vereshchetin supports that space law rules are space-, function-, and time-oriented, hence are designed for application not only in space, but also on the Earth. The rules should be observed before the launch and while the object is in outer space.

15 J Hermida, *Legal basis for a national space legislation* (Space Regulations Library, Kluwer Academic Publishers 2004) 29–32.

16 A concise overview of the main elements and procedures of national authorisation can be found in I Marboe, F Hafner, 'National authorisation mechanisms in implementation of the UN treaties' in F G von der Dunk (ed), *National space legislation in Europe* (Studies in Space Law vol 6, Brill 2011) 46-68. A comparative analysis of the main elements of various national space laws can be found in A Froelich, V Seffinga (eds), *National space legislation – A comparative and evaluative analysis* (Studies in Space Policy vol 15, Springer 2018) 137-186.

partly or wholly covered by the authorisation and supervision provisions of Article VI OST.

The connection between a State and a private entity is important considering that space big data applications are often performed by companies situated in more than one State and that they are made available in several countries around the world.

3.1.3 Registration of space objects

Except for international responsibility, authorisation, and supervision, the link between States and the activities of public and private actors is further strengthened by the duty to register space objects. Article VIII OST mentions that States shall retain jurisdiction and control over the launched objects that are registered in their national registries.[17] However, the obligation to proceed with such formality is only established by the Registration Convention. In Article II, the Registration Convention imposes on its member States the duty to register the objects they have launched into outer space. Before this requirement, Article I specifies that the States bearing such obligations are the ones that launch or procure the launching, as well as those from whose territory or facility an object is launched. The Convention also provides for the registration of objects that have been jointly launched by more than one State,[18] as well as the ones that are launched by international organisations.[19] Apart from filing with the respective national registry, States should provide details concerning their launched objects to the UN Secretary-General, who also maintains an international registry with full and open access to the information contained therein.[20] As far as the registered information is concerned, Article IV REG sets out a list of specifications, which include technical elements as well as the general function of the launched object. According to Article VII, these provisions also apply to international intergovernmental organisations.

In the framework of space big data, the Registration Convention applies to satellites that are launched with the purpose, exclusively or among others, of collecting, storing, and disseminating data.

The Resolution on registering space objects[21] provides further recommendations to States and international intergovernmental organisations, in

17 The way in which jurisdiction and control over space objects can be exercised by their State of registry can be found in B Cheng, 'The commercial development of space: The need for new treaties' (1991) 19 JSL 17, 33 and 37.

18 REG (n 5) art II.2.

19 REG (n 5) art VI.1.

20 REG (n 5) art III and IV.

21 UNGA Res 62/101 (10 January 2008) Recommendations on enhancing the practice of States and international intergovernmental organizations in registering space objects UN Doc A/RES/62/101.

order to better implement the provisions of the Registration Convention.[22] In particular, it suggests harmonising the information that is furnished to the UN Secretary-General. Further detailing the provisions of Article IV REG, the Resolution proposes the use of uniform measurement systems and additional information regarding the registered space objects. The Resolution also gives recommendations to overcome hurdles in registration by international intergovernmental organisations and in joint launches. In cases where an international intergovernmental organisation has not declared acceptance of the Registration Convention and there is no consensus regarding registration among its members, an alternative solution should be sought. This is a pertinent provision, given the role of organisations in the launching and operation of EO and GNSS satellites that generate and transmit space data. In cases of joint launches, the Resolution suggests that the State from whose territory or facility an object is launched contacts other States that also qualify as launching States, in order to arrange the proper registration of the space object. Moreover, when several space objects are launched, the State responsible for each object, according to Article VI OST, should ensure the registration of the object. These recommendations can alleviate some of the concerns regarding registration when several States can be identified as launching States. Indeed, it is often the case that a satellite involved in a space big data system is launched from the territory or facility of a different State than the State that procured the launch. For example, a satellite can be procured in the State where its manufacturer is located, but launched from the territory of another State that has launching capabilities. Even though the Resolution on enhancing registration practices is not binding, it can serve as guidance for States and international organisations in implementing their duty to register the space objects they launch.

Overall, the registration of space objects is essential, in order to determine the State that exercises jurisdiction and control upon them and to identify the State(s) that are liable for damages caused by space objects. The UN Office for Outer Space Affairs reports that over 86% of the objects in orbit and beyond are registered with the UN Secretary-General.[23]

22 An explanation of the provisions of the Resolution can be found in T Masson-Zwaan, 'Registration of small satellites and the case of The Netherlands' in I Marboe (ed), *Small satellites-Regulatory challenges and chances* (Studies in Space Law vol 11, Brill 2016) 181-182.

23 UN Register of Objects Launched into Outer Space <https://www.unoosa.org/oosa/en/spaceobjectregister/index.html>. All links in this chapter were last accessed on 2 December 2023; An online index of objects launched into outer space is available at <https://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id=>. The index includes over 16.973 objects, of which over 15.295 objects are registered with the UN as of 1 December 2023.

3.1.4 Liability for damage from space activities

The Outer Space Treaty provides for international liability of the launching State for damages caused to another State by its launched object. This provision has been further elaborated in the Liability Convention which introduces definitions of the basic terms, distinguishes among different types of liability, and sets out the requirements for the attribution of liability to States.

The definition of a 'launching State' in Article I LIAB is the same as the one provided in Article I of the Registration Convention, namely the State that launches or procures the launching or the State from whose territory or facility an object is launched.[24] In addition, the term 'damage' is defined in Article I as the loss of life, personal injury, or other health impairment, as well as the loss or damage to property, suffered by States or natural and legal persons. Finally, according to Article I, a 'space object' includes the component parts of a space object, its launch vehicle, and parts thereof.[25]

In the context of space big data, the satellites involved in the collection, storage, and transmission of data fall under the definition of a space object. As per Article II LIAB, in case of damage caused on the Earth, the launching State bears absolute liability, whereas Article III LIAB prescribes fault liability for damages elsewhere than on the surface of the Earth, as damages to other space objects or property on board of it. The Liability Convention covers damages 'caused by' space objects, so a causal link between the object in question and the damage is required.[26] However, scholarly opinions differ regarding whether the causation between the space object and the damage should be direct or it suffices to be indirect.[27] The view that the purpose of

---

24 The special regime of the launching State for launches from the Baikonur cosmodrome in Kazakhstan, which is leased to Russia and is based on the Russia-Kazakhstan Treaty on the Leasing of the Baikonur complex, is explained in G Zhukov, 'Can the State from whose territory a space object is launched declare itself a non-launching one?' (2003) 28.1 ASL 50, 51-53.

25 S Gorove, 'Toward a clarification of the term space object – An international legal and policy imperative?' (1993) 21 JSL 11, 13-14 and 25-26. Neither LIAB (n 4) nor REG (n 5) define the term 'space object', other than by reference to an 'object'. Their scope, as also seen in their preparatory work, indicate that the ordinary meaning of an object should be used. Based on that, an object is a material thing that can be seen or touched and is in stable form, and does not include anything intangible, such as a satellite signal.

26 It has been supported that the characterisation of 'caused by' as covering direct or indirect damages does not affect the way in which liability is determined. W F Foster, 'The Convention on International Liability for Damage Caused by Space Objects' (1972) 10 Canadian Yearbook of International Law 137, 158.

27 Christol explains the meaning of direct and indirect damage in the text of the OST and the LIAB, taking into account the negotiation of the treaties and potential scenarios of damage. He notes that it remains unclear whether the treaties cover direct or also indirect damage, which remains a subject of interpretation. C Q Christol, 'International liability for damage caused by space objects' (1980) 74.2 American Journal of International Law 346, 358-362. Carpanelli and Cohen observe that the ordinary meaning of the provisions of LIAB points to a narrow interpretation of damage that covers only those that are directly

the Liability Convention is to cover direct damage and not extend to indirect damage, prevails. Indirect damages that are not foreseen by the Liability Convention include, for instance, damages caused by satellite signal, such as the one used to receive and transmit space data. By that account, it is difficult to construct a case for absolute or fault liability for space big data activities and applications, since direct damage is not the type of damage caused by space big data. A relevant example can be seen in the case where SSA data, one of the identified types of space data, are used in an automated way, based on the features of big data, for collision prediction and avoidance.[28] Physical damage occurring due to the collision of space objects as a result of an error in the collection, use, or dissemination of data can be used as an example since it involves a close connection between the data and the damage. Even so, the provisions of the Liability Convention may be difficult to justify, since the damage would not have been caused by a space object. With this in mind, potential damages caused by space big data, such as damages from data transmission, false data, or cyber incidents, are not explicitly covered by the Liability Convention, since they do not constitute direct damage on the Earth or in outer space. To support the argument regarding limited liability for data uses, except for interpreting the provisions of the Liability Convention, the terms concerning the use of space data can also be taken into account. For instance, the EU Space Programme Regulation explicitly provides no warranty of quality and accuracy, as well as reliability, speed, and suitability, for the data provided by the Programme's components.[29] In the case of SSA data,

caused by a space object. Although, they proceed counterarguing that a narrow interpretation may not have been the goal of the drafters of LIAB, a wider interpretation that encompasses damages from space data does not appear to be that goal either. E Carpanelli, B Cohen, 'Interpreting 'damage caused by space objects' under the 1972 Liability Convention' in C M Jorgenson (ed), *Proceedings of the International Institute of Space Law 2013* (Eleven International Publishing 2014) 34. That is also supported by Kong in his analysis of liability for GNSS signal, where he looks into different interpretations of whether signal can be considered a space object that caused damage and notes three approaches. The first approach is that a space object should have material and physical properties, unlike signal. The second approach is that damage from signals is not entirely excluded from LIAB and the third approach accepts that signals fall under the term space object. After examining the preparatory work of LIAB, he concludes that the drafters of international space law did not intend to include signal in the definition of space objects for the purpose of liability. D Kong, *Civil liability for damage caused by global navigation satellite system* (Aerospace Law and Policy Series vol 15, Kluwer Law International 2018) 72 and 77.

28 S A Kaiser, 'Legal and policy aspects of space situational awareness' (2015) 31 Space Policy 5, 10. The relevance of international space law provisions in general to space situational awareness is explained in M Borowitz, 'Legal considerations and future options for space situational awareness' (2020) 48 Georgia Journal of International and Comparative Law 695, 698-701.

29 Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Agency for the Space Programme and repealing Regulations No 912/2010, No 1285/2013, No 377/2014, and Decision No 541/2014/EU [2021] OJ L 170/69 art 10 (hereinafter EUSPA Regulation).

the providers of SSA data and services also waive liability for the use of their data.[30]

In cases where damage is caused by signals or ground-based objects, instead of space objects as required by the Outer Space Treaty and the Liability Convention, liability can be claimed through other means, such as product liability and public international law.[31] In the former case, liability can be claimed if one of the products involved in the space big data process, such as a satellite sensor or a signal receiver, did not function as expected. In the latter case, liability can be construed, if a State is found to have violated one of its international obligations, such as the duty of Article IX OST to consult before proceeding with activities that may interfere with space activities that generate space big data or engaging in activities that affect the cybersecurity of the space big data lifecycle and breach international obligations in this regard. Besides, the Resolution on the application of the concept of the 'launching State'[32] encourages States to adopt national laws for the authorisation and supervision of their space activities, in fulfilment of their obligations under, among others, the Liability Convention. National laws may provide clarity as to how damages caused by space activities are treated by the States that licensed them.

3.1.5 Harmful interference with activities in outer space

Article IX OST includes several conditions according to which States should conduct their activities in outer space. In its first sentence, it provides that States should be guided by cooperation and mutual assistance in their space activities and that they should pay due regard to the corresponding interests of other States parties. This principle reflects the interoperable character of space big data, which relies on cross-border data transfer and collaboration among missions that collect space data.

---

30 The example of a user agreement for Space-Track.org, a catalogue of space objects created by the Aerospace Corporation can be found in <https://www.space-track.org/documentation#/user_agree> and <https://aerospace.org/ssi-space-situational-awareness>.

31 A Loukakis, 'Product liability ramifications for damage caused by erroneous GNSS signals' in M Hofmann (ed), *Dispute settlement in the area of space communication: 2nd Luxembourg workshop on space and satellite communication law* (Nomos/Hart 2015) 183-199; A Loukakis, *Non-contractual liabilities from civilian versions of GNSS – Current trends, legal challenges and potential* (Nomos, 2017) 235-239. According to Article III OST, States should carry out their activities in accordance with international law, which also entails provisions regarding the liability of States for damage caused due to a wrongful act attributable to them, in the form of reparation. International law liability mainly stems from the 2001 Articles on State Responsibility for Internationally Wrongful Acts UN Doc A/RES/56/83, Articles 1, 2, and 31. *See* also B Cheng, *Studies in international space law* (OUP 1997) 611-612.

32 UNGA Res 59/115 (25 January 2005) Application of the concept of the 'launching State' UN Doc A/RES/59/115.

Article IX OST, in its fourth sentence, calls upon States to consult, before proceeding with activities that cause potentially harmful interference with the activities of other States. The term 'interference' is not defined in the text of the treaty, but can be interpreted through its ordinary meaning.[33] Accordingly, interference can appear in the form of electronic interference, when a satellite signal is affected, kinetic interference, when a space object is physically affected, as well as any other activity that impacts satellite communication.[34] Interference is relevant to space big data, as it may affect the collection and dissemination of data, should a satellite system face disruptions in its operation in outer space. Even when interference is defined though, Article IX OST does not provide for adequate protection, since a State would first have to determine whether interference is harmful, before determining whether it is potentially harmful and, ultimately, proceeding with consultations.[35]

Harmful interference also appears in the instruments of the International Telecommunications Union (ITU), where it is described and regulated concretely. The ITU Constitution provides for fundamental principles for telecommunications, the ITU Convention includes operational procedures, and the ITU Radio Regulations include provisions for avoiding harmful interference.[36] The purpose of the ITU is to improve and rationalise the use of telecommunications, to ensure the efficiency, usefulness, and availability of telecommunication services, and to harmonise the actions taken to fulfil its purposes.[37] The ITU has a broad range of competencies, to meet its aforementioned purposes.[38] Primarily, ITU is in charge of allocating bands for the radio-frequency spectrum, allotting radio frequencies, registering frequency assignments, and eliminating harmful interferences between radio stations of different countries. Moreover, it works toward improving the use of spectrum for radio-

33 Vienna Convention on the Law of the Treaties (opened for signature 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331 art 31.1.

34 Types of interference as described by F von der Dunk, 'The 'space side' to 'harmful interference' – Evaluating regulatory instruments in addressing interference issues in the context of satellite communications' in M Hofmann, *Legal rules for interference-free radio communication: 3rd Luxembourg workshop on space and satellite communication law* (Nomos/Hart 2015) 89.

35 J F Mayence, 'Harmful interference in telecommunications' in M Hofmann, *Legal rules for interference-free radio communication: 3rd Luxembourg workshop on space and satellite communication law* (Nomos/Hart 2015) 103-104.

36 Constitution of the International Telecommunication Union (as amended in 2022) (hereinafter ITU Constitution), Convention of the International Telecommunication Union (as amended in 2022), International Telecommunication Union Radio Regulations (2020) (hereinafter ITU Radio Regulations). A concise description of the role of the ITU in regulating satellites can be found in A L Allison, *The ITU and managing satellite orbital and spectrum resources in the 21st Century* (Springer Briefs in Space Development, Spinger 2014) 17-24.

37 ITU Constitution (n 36) art 1.1.

38 ITU Constitution (n 36) art 1.2.

communications,[39] standardising the quality of telecommunications, harmonising the development of telecommunication facilities, and promoting cooperation and exchange with less developed countries.

The role of the ITU affects space big data in that satellites that collect, store, and transmit data should comply with its rules. In particular, as far as the radiofrequency spectrum and orbits are concerned, the ITU calls for its Member States to limit the number of frequencies and spectrum to the minimum essential to provide quality services.[40] It also establishes that radio frequencies and associated orbits are limited natural resources and must be used rationally, efficiently, and economically, according to the Radio Regulations.[41] As far as harmful interference is concerned, stations should be established in a manner that does not cause harmful interferences with radio services communications.[42] Furthermore, each State should ensure compliance with the non-interference provisions and take all practical measures to prevent interference.[43] Harmful interference is defined as interference that endangers the functioning of radionavigation or other safety service or interference that seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service.[44] In that sense, the provisions of the ITU offer concrete protection to satellite systems involved in the space big data lifecycle that use radiocommunication signals. The allocation of frequency bands and the allotment of radio frequencies are part of the ITU Radio Regulations.[45]

The concept of harmful interference in the ITU Constitution is different from the one in Article IX OST. The harmful interference concept in the context of the ITU is clearly defined and should be explicitly avoided. Harmful interference in the OST is not defined, whereas it is also not prohibited. States should consult in case their activities can cause potentially harmful interference. Despite its vague language though, when given appropriate interpretation, Article IX OST can cover other types of interference than only signal inter-

39 The Annex of the ITU Constitution (n 36) in line 1009 defines radiocommunications as telecommunications by means of radio waves. In line 1005, it includes the same definition with further specification of radio waves that are electromagnetic waves of frequencies arbitrarily lower than 3000GHz, propagated in space without artificial guide.

40 ITU Constitution (n 36) art 44.1 and ITU Radio Regulations (n 36) art 4.1.

41 ITU Constitution (n 36) art 44.2.

42 ITU Constitution (n 36) 45.1. Stations, according to the ITU Radio Regulations (n 36) art 1.61, are 'one or more transmitters or receivers or a combination of transmitters and receivers, including the accessory equipment, necessary at one location for carrying on a radiocommunication service, or the radio astronomy service'.

43 ITU Constitution (n 36) art 45.2 and 45.3.

44 ITU Constitution (n 36) annex line 1003.

45 The ITU Regulations (n 36), in Article 1.16 provide for the entry of frequency bands in the table of frequency allocations in order to be used. Article 1.17 provides for the entry of a designated frequency channel in an agreed plan, in order for a radio frequency to be allotted. According to Article 1.18, authorisation is given by a national administration in order for a radio station to use a frequency or a channel. Frequency assignments should be brought into use within 7 years from the notification of the ITU, as per Article 11.44.

ference as in the case of the ITU, and can thus prevent a wider type of disruptions.

3.1.6 Preliminary conclusions on the connection between international space law and space big data

In the framework of space big data, the provisions of the international space treaties find general application but do not have a direct legal effect on the collection, access, use, and dissemination of space big data of either of the four space data categories, EO data, GNSS data, satellite-based internet data, or astronomy and other data related to space. Especially regarding the latter, the international space treaties do not find application to activities that may form part of the space big data lifecycle but are not connected to systems found in outer space, such as the collection of astronomy and SSA data by ground-based sensors.[46]

The freedoms of outer space, enshrined in Article I OST, enable the launch and operation of missions that collect and disseminate space big data. Given the various civil and commercial uses of space big data, these missions, and space big data applications in particular, help realise the sharing of benefits from space activities among countries, as is also envisioned in Article I OST.

A unique parameter in the regulation of space activities that affects both the regulation and application of laws on space big data is the lack of national sovereignty in outer space, as laid down in Article II OST. The application of national, regional, and international laws is tied to the notion of national sovereignty, which dictates which law is applicable within a certain State. Without national sovereignty, the application of laws that are analysed in the following sections can be questioned. Nevertheless, links between the activities carried out in outer space and a State can be established irrespective of the lack of national sovereignty in outer space. First, according to Article VI OST, States are internationally responsible for their national activities in outer space, which they should authorise and supervise. By means of Article VI, States adopt national regulations regarding the licensing and operation of space activities, including the activities that are part of the space big data lifecycle. These regulations include conditions set by the State and applied to its national space activities; hence they may also cover the collection, access, use, and dissemination of space big data. Second, Article VIII OST, as further elaborated

46 The application of the space treaties in this scope is contentious, as can be seen in the example of interference that satellite constellations cause to ground-based astronomy. The International Astronomical Union has launched the initiative of Dark and Quiet Skies <https://www.iau.org/public/darkskiesawareness/> and has raised the matter with UNCOPUOS, Recommendations to Keep Dark and Quiet Skies for Science and Society (19 April 2021) UN Doc A/AC.105/C.1/2021/CRP17.

in the Registration Convention, dictates that the State of registry of a space object, such as the objects that collect, store, and disseminate space big data, retains jurisdiction and control over that object. Jurisdiction and control confer to States the authority to enforce their laws and determine the activities of their registered objects.

Finally, in the scope of the UN Space Treaties, the provisions regarding liability and harmful interference may find application in space big data. Article VII OST and the Liability Convention foresee liability of the launching State for damages caused to and from an object that can be involved in the space big data lifecycle. Such damage can have an impact on the collection, access, use, and dissemination of space big data. The same may apply to the impact of harmful interference caused by objects collecting, storing, or disseminating space big data, as described in Article IX OST.

The UN Space Treaties were adopted to govern the activities of States in outer space and took into account the contemporary state of space technology at the time of their adoption. Even though the premises upon which international space law was built have evolved, the space law principles still find application in space big data, since they introduce another dimension to their regulation and are transferred to domestic space legislation, thus affecting collection, access, use, and dissemination. In this regard, they apply to all the identified types of space data, namely EO data, satellite-enabled location data, space-based connectivity data, as well as astronomy data, and other data related to space.

Telecommunication rules that apply to space activities have the most relevance to space big data, as far as international space law is concerned. This is because the instruments of the ITU govern the operation of satellites, including the reception and transmission of their signal, which in turn affects access and dissemination of space data. Furthermore, they establish the main rules for the placement in orbit and operation of the satellites involved in the space big data lifecycle, such as the allocation of frequencies and orbital slots and the prohibition of harmfully interfering with other space activities.

3.2 Privacy and data protection law

Digital data, such as space data, encompass information of various sorts and content. Whereas some of this information is generic or of no particular significance, other parts might refer to personal details or issues of a private nature. This kind of personal data forms the basis of the concepts of privacy and data protection, which have become particularly relevant, especially given the increasing reliance on data for various uses and applications. The realisation of the benefits and potential of data stems from the diversity of its content, which can be deployed for different purposes. The case for the benefits of space data has been analysed in section 2.1.3. At the same time though, the growing

demand for data leads to growth in the generation, collection, transfer, and use of data, and consequently to challenges in maintaining a sufficient level of privacy and data protection, as prescribed in laws that include specific collection and distribution requirements.

The right of persons to the protection of their personal information has been established in international law and has been transferred to several regional and national regulations. This right of individuals is the focus on this section, which examines privacy and data protection in the scope of space big data and the connection between space big data and personal data. Section 3.2.1. elaborates on the right to privacy and data protection, as shaped in the EU regulatory framework, followed by a brief analysis of the equivalent regime in the US, given the involvement of US entities in space big data. Sections 3.2.2 and 3.2.3 address data protection through the lens of space big data, particularly concerning high-resolution EO data, location data, and satellite-based connectivity data.

3.2.1 The EU regulatory framework on privacy and data protection

Privacy is an internationally recognised fundamental right. It appeared in the Universal Declaration of Human Rights of 1948 as the right of individuals to not be subjected to interference with their privacy and legal protection against such interference.[47] It is also among the provisions of the European Human Rights Convention of 1950, which similarly proclaims the right to respect the private life of individuals and to non-interference by public authorities.[48] Privacy is closely associated with data protection and the terms are often used interchangeably. The former establishes the regulatory obligation to preserve the privacy of individuals, whereas the latter establishes mechanisms to achieve this goal. The right to privacy limits the involvement of a State in the affairs of those under its jurisdiction and ensures that a State does not interfere with their private matters. It is translated into data protection laws that safeguard the personal information of individuals from being unlawfully used. National and regional laws offer different levels of protection of personal data. Their common characteristics include the control (e.g., through consent) of data subjects over the processing of their data, the use of personal data for predefined purposes, and their transfer only subject to specific predefined conditions. Exceptions are in place for the use of personal data by governments and reasons of public interest. Upon those premises, the conjunction between privacy, data protection, and space big data is examined. The scope of pro-

47 Universal Declaration of Human Rights (1948) art 12.

48 European Convention for the Protection of Human Rights and Fundamental Freedoms (opened for signature 4 November 1950, entered into force 3 September 1953, as amended by Protocols 11 and 14) ETS 5 art 8.

tection of the EU framework on data protection, the rights and obligations it creates and how it compares with the equivalent US regime are addressed in the sections below.

– *The scope of protection of the EU privacy and data protection framework*

In the EU, data protection takes a central place in the regulatory scene. The EU Charter of Fundamental Rights refers to the protection of personal data, which should be processed fairly, for specified purposes, and upon consent of the concerned person or on a legitimate basis.[49] The Treaty on the Functioning of the European Union establishes the right of every citizen to the protection of their data,[50] and the Treaty of the European Union calls for the EU Council to adopt decisions on rules concerning personal data concerning their processing and their free movement.[51] The EU General Data Protection Directive (GDPR)[52] lays down detailed provisions regarding the legitimacy and lawfulness of the processing of personal data. It was adopted in 2016 and came into force in May 2018, becoming directly binding for all EU Member States. The purpose of the Directive is to safeguard personal data[53] from processing by automated means or when forming part of a filing system.[54] It applies to data controllers and data processors established in the EU, even if the processing does not take place in the EU, as well as to the personal data of subjects in the EU, making its scope rather broad.[55] The GDPR creates rights for data subjects over their personal data and obligations for data controllers and processors. In this framework, personal data refer to information that relates to an identified or identifiable person.[56] A person is identifiable when they can be identified, directly or indirectly. Examples of identifiers mentioned in the definition of personal data are the name, location data, online identifiers, or factors specific to the economic and social identity of people.

The GDPR governs the processing of personal data, namely the set of operations performed on personal data, by automated or non-automated means.[57] These operations include a wide range of data handling methods, such as collection, organisation, structuring, storage, adaptation, retrieval, use,

49 Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 art 8.
50 Treaty on the Functioning of the European Union (consolidated version) [2012] OJ C 326/47 art 16 (hereinafter TFEU).
51 Treaty on European Union (consolidated version) [2012] OJ C 326/13 art 39.
52 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 their personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (hereinafter GDPR).
53 GDPR (n 52) art 1.1.
54 GDPR (n 52) art 2.1.
55 GDPR (n 52) art 3.
56 GDPR (n 52) art 4.1.
57 GDPR (n 52) art 4.2.

disclosure by transmission, dissemination, making data available, and a combination of data. They are also present in every part of the space big data lifecycle, as described in section 2.1.2. Therefore, the GDPR can find application on space big data, whenever the latter include personal data.

– *The rights and obligations under the EU privacy and data protection framework*

The GDPR imposes specific requirements on data controllers and data processors for the processing of personal data that are laid down in Article 5. These requirements, also referred to as principles of data processing, include lawfulness, fairness, and transparency of data processing; purpose limitation of data collection and processing; data minimisation; data accuracy; storage limitation; and data integrity and confidentiality. Given the uses of space data, which are different from the uses for which these principles were introduced, the requirements for fairness and transparency are not closely relevant. On the other hand, lawfulness of data processing, the purpose limitation, the data minimisation, and the storage limitation affect the collection of, access to, and use of data and hence are deemed of particular relevance to space data. The lawfulness of data processing requires the consent of the data subject, the performance of a contract to which the data subject has agreed, the fulfilment of a legal obligation of the controller, public interest or official authority, or legitimate interests pursued by the controller.[58] This requirement may significantly limit the collection of space data if these data are personal. The purpose limitation entails the collection of personal data for specific purposes and their processing strictly within these purposes.[59] Connected to the purpose limitation is the minimisation of collected data to only those that are essential for performing the purposes for which they are collected.[60] The purpose limitation and data minimisation may affect the use of space data that are personal data. This is because the advantages of space data include the ability to use the same data for various purposes that are not pre-determined. Similarly, data should be preserved only for the period that is necessary to fulfil the purpose for which they were collected.[61] Although this may affect the use of space data, the GDPR does not prescribe specific time limitations for data storage. Therefore, this requirement is not further addressed in section 3.2.

These requirements are incumbent on the data controller, namely the natural or legal person, or public authority, or agency, or other body that determines the purpose and means of processing personal data, alone or jointly

58 GDPR (n 52) art 6.1.
59 GDPR (n 52) art 5.1(b).
60 GDPR (n 52) art 5.1 (c).
61 GDPR (n 52) art 5.1 (e).

with others.[62] The data controller should implement technical and organisational measures that should be reviewed accordingly[63] and will be implemented by design and by default.[64] When the controller delegates the processing to a data processor, the latter should guarantee similar compliance.[65] A processor is a natural or legal person, or public authority, or agency, or other body that processes personal data on behalf of the controller.[66] Any cooperation between the processor and other processors should be subject to prior authorisation of the controller and carried out under specific agreed terms.[67]

– *A comparison with the US privacy and data protection framework*

Whereas the GDPR establishes a comprehensive privacy framework with detailed data protection provisions, the equivalent US framework is fragmented and of significantly different scope.

The Fourth Amendment to the US Constitution establishes the right of individuals to be secure in their private confinements.[68] A number of federal and state regulations further outline the specific privacy provisions. The US Privacy Act of 1974 includes provisions regarding data held by governmental agencies and conditions for their lawful collection, storage, use, and dissemination. The term 'personal data' is not explicitly defined in the Act. Instead, the Act protects information regarding individuals, meaning citizens of the US or aliens lawfully admitted for permanent residence.[69] The main premise of the US Privacy Act is the 'no disclosure without consent' requirement for sharing information about individuals with third parties. A list of exceptions from this requirement includes twelve instances, related to formalities and law enforcement, where consent is not required. The US regime on privacy is different than its EU counterpart, in that it does not comprise uniform legislation that is applicable throughout the USA.[70] Therefore, data protection requirements may vary among the fifty States, and essential terms, such as personal data, data controller, and data processing may not be as clearly

62 GDPR (n 52) art 4.7 and 24.
63 GDPR (n 52) art 24.1.
64 GDPR (n 52) art 25.
65 GDPR (n 52) art 28.
66 GDPR (n 52) art 4.8.
67 GDPR (n 52) art 25.2, 25.3, and 25.4.
68 United States Constitution (as amended), amend IV. The first analysis of the right to privacy in US legal theory, described as the right to be left alone, is conducted in S D Warren, L D Brandeis, 'The right to privacy' (1890) 4.5 Harvard Law Review 193, 205.
69 5 USC § 552 art a(a)(2).
70 A general overview of the status of privacy laws in the US can be found in 'Data protection laws of the world' (*DLA Piper*, 29 January 2023) <https://www.dlapiperdataprotection.com/index.html?t=law&c=US> and a summary of recent developments in this field is provided in H Vrabec, 'The US privacy déjà-vu' (*Leiden Law blog*, 31 January 2023) <https://www.leidenlawblog.nl/articles/the-us-privacy-deja-vu>.

described as in the EU regime. Except from this general piece of legislation, data protection is regulated individually by the fifty US states; each may introduce its data protection laws. However, terms such as 'data controller', 'data processing', or 'personal data' are not defined therein. Furthermore, there are several sector-specific privacy regulations in the US, such as the Gramm-Leach-Bliley Act concerning personal financial information, the Health Insurance Portability and Accountability Act (HIPAA) that relates to personal health information, and the Children's Online Privacy Protection Act (COPPA) that protects personal information of children younger than twelve years.[71]

Moreover, the right to privacy in the US is also viewed through the lens of the presence of the data subject in the public domain. In particular, the 'reasonable expectation of privacy' test examines whether the data subject exhibits an expectation of privacy and whether this expectation is largely seen as reasonable.[72] The test has been used in cases where legal proceedings against an individual were instituted, using GPS data, which is personal data and a type of space data, that have been collected without a warrant.[73] In some occasions, these data were admitted to the court, although they were collected or used without the knowledge or agreement of the data subject, because they may have concerned activities that took place in a public area, where a person should not reasonably expect to maintain their privacy.

3.2.2 Privacy in the scope of space big data[74]

The relevance of privacy and data protection to the use of space big data is twofold. First, space big data may directly comprise or incorporate personal data, namely data that identify or can identify a person, such as location data enabled by satellite and online identifiers included in satellite-based connectivity data. Second, the combination of non-personal data through space and big data may result in information that can identify individuals and hence

71 Gramm-Leach-Bliley Act of 1999, Health Insurance Portability and Accountability Act of 1996, Children's Online Privacy Protection Act of 1998.

72 The reasonable expectation of privacy test was introduced in the Katz v. US case. Katz v United States [1967] 389 US 347. In Rakas v. Illinois, the Supreme Court found that the reasonable expectation of privacy test should be connected to sources outside the Fourth Amendment. Rakas v Illinois [1978] 439 US 128. Similar was the reasoning in Gonzales v Uber Technologies, Inc. [2018] 305 F. Supp 3d 1078 and United States v Haqq [2002] 213 F. Supp 2d 383.

73 R McDonald Hutchins, 'Tied up in knotts? GPS technology and the Fourth Amendment' (2007) 55 UCLA Law Review 409, 445-452. The author provides a thorough analysis of the grounds of the reasonable expectation of privacy test in conjunction with the use of GPS data obtained without a warrant in court in various cases decided by US courts.

74 Part of the analysis in section 3.2.2 has been published in D Stefoudi, 'Space data in the fight against pandemics: Privacy concerns and sharing of benefits from the use of space technology for decision-making' (2020) 45 (special issue) ASL 108.

constitute personal data. Therefore, to determine whether data protection regulations apply to space big data, creating obligations for controllers and processors, the first step is to address the question of whether personal data is involved in any stage of the space big data lifecycle, which is described in section 2.1.2.

In the field of *EO data*, the increasing quality of pictures taken by satellites can pose privacy concerns.[75] For example, satellite images of 30cm resolution can reveal the location of vehicles on the ground, whereas 25cm resolution enables detailed object classification (figures 2.5, 2.6, 2.7, 2.8, 2.9). Both resolutions are commercially available in the form of satellite data packages, as well as in the form of analysed data products.[76] However, the direct identification of individuals through these resolutions may not be possible.[77] It may be rendered feasible though, as the quality of remote sensing images improves to resolutions closer to 10cm.[78] At the same time, the processing of available high-resolution images through data fusion and calibration may facilitate the identification of individuals. Therefore, personal data may become part of space

75 S Erwin, 'Lawmaker warns remote sensing industry could be challenged by security and privacy issues' (*Space News*, 17 March 2021) <https://spacenews.com/lawmaker-warns-remote-sensing-industry-could-be-challenged-by-security-and-privacy-issues/>; E Dans, 'Satellite surveillance: nowhere is private anymore' (*Medium*, 8 July 2019) <https://medium.com/enrique-dans/satellite-surveillance-nowhere-is-private-anymore-172718e34f37>; C Beam, 'Soon, satellites will be able to watch you everywhere all the time – Can privacy survive?' (*Technology Review*, 26 June 2019) <https://www.technologyreview.com/2019/06/26/102931/satellites-threaten-privacy/>; S Parcak, 'Are we ready for satellites that see our every move?' (*The New York Times*, 15 October 2019) <https://www.nytimes.com/2019/10/15/opinion/satellite-image-surveillance-that-could-see-you-and-your-coffee-mug.html>; S Shufelt, 'Remote sensing satellites and privacy: Why current regulations will ultimately fail' (*American University Business Law Review*) <https://aublr.org/2020/03/remote-sensing-satellites-and-privacy-why-current-regulations-will-ultimately-fail/>

76 An example of the difference between resolution of 10m, 1m and 30cm can be found in 'True 30cm VHR imagery' (*European Space Imaging*) <https://www.euspaceimaging.com/true-30-cm-imagery/>. The map on the website of Maxar allows the user to view the highest resolution available through that company, which can depict very accurately buildings and vehicles. https://www.maxar.com/products/optical-imagery. Resolutions between 30 and 50cm present similar results <https://planetobserver.com/vhr-imagery/>. Currently, ICEYE offers 25cm Synthetic Aperture Radar (SAR) resolution, which is able to detect minor changes on the ground. P Laurilla, 'New benchmark in imaging from SAR microsatellites: ICEYE presents 25cm Azimuth resolution' (*ICEYE*, 2 April 2020) <https://www.iceye.com/blog/new-benchmark-in-imaging-from-sar-microsatellites-iceye-presents-25-cm-azimuth-resolution>.

77 Although it is argued differently, technology has not evolved to that level, by the time this thesis is written. *See* E Wanshel, 'Google's satellites could soon see your face from space' (*Vice*, 11 August 2014) <https://www.vice.com/en/article/8qx54b/googles-satellites-could-soon-see-your-face-from-space>; K Tatera, 'New satellites will detect your face and phone from space' (*The Science Explorer*, 15 October 2015) <http://thescienceexplorer.com/technology/new-satellites-will-detect-your-face-and-phone-space>.

78 D Werner, 'Albedo wins license to sell 10-centimeter imagery' (*Space News*, 14 December 2021) <https://spacenews.com/albedo-wins-license-to-sell-10-centimeter-imagery/>

big data, especially given the abundance of information and analytical capabilities that space big data enable. The same is the case with radar remote sensing images, especially of high resolution, that enable the detailed classification of objects on the ground and the detection of changes.[79]

Whether space data contain personal data depends on their type. EO data have the potential to contain personal data if personal information can be extracted from them. In turn, that depends on whether the resolution of EO data is high enough to directly identify individuals or whether EO data can identify individuals.

GNSS data are personal data since location is one of the categories of data that make an individual identifiable. Information regarding the location and movement of people is used in a great number of applications, as described in chapter 2. Tracking the location and movement of people relies on the constant acquisition of real-time geolocation information that is enabled by space technology, namely by Global Navigation Satellite Systems, and that allows remote monitoring of individuals simultaneously and for limitless periods. It also enables the identification of the location of individuals at specific moments, in an accurate and resourceful manner.[80] Location data derive from mobile devices with built-in receivers that use navigation satellite signals to track their geographical position at given times. Satellite geolocation relies on the GNSS receiver of the device, where data transmitted by satellites are used to calculate the location of the device. The receivers of navigation signals are passive, in that they simply receive and translate the information that is continuously transmitted by GNSS satellites. Given that satellites do not collect location information, space data in the form of GNSS signals do not include personal data. Instead, location data is collected and processed by the receivers on devices that support geolocation applications, which would not function as accurately without the use of satellite navigation.

The issue of data protection also arises in the case of *satellite-based internet connectivity*, when personal information is included in the internet traffic data that is circulated via satellite signal among various devices. Similar to GNSS signal, only after the signal is received by a device it is translated to information that may include personal data. Therefore, the connection between satellite-based internet data and personal data can be viewed under two circumstances, depending on whether space big data includes personal data. On the first occasion, space big data may simply enable the transfer of signal via satellite-based internet, which is transformed into data, potentially including personal information, by a receiving device outside the space big data lifecycle, such as an individual's smartphone or other electronic device. There, it can be concluded that space big data do not include personal information, as they

79 J Atli Benediktsson, J Chanussot, W M Moon, 'Very high-resolution remote sensing: Challenges and opportunities' (2012), 100.6 Proceedings of the IEEE, 1909 (June 2012).

80 (n 73).

only facilitate the transmission of a signal to a device outside the space big data lifecycle. On the second occasion, the information transmitted via satellite-based internet, potentially including personal information, forms part of the space big data lifecycle, since it is this information that is collected, processed, used, and disseminated within the cycle. This distinction determines the condition for the lawful processing of personal information, especially in terms of the consent of the data subject, as will be examined below.

In the case of *astronomy and other space-related data*, the issue of data protection does not appear relevant, as these data do not include personal information.

3.2.3 The application of data protection laws to space big data

The application of data protection laws to space big data depends on whether space big data include personal data, meaning information that identifies or can identify an individual. Given the amount of available data and the various levels of processing that space big data undergo, the determination of whether space data include personal information may prove cumbersome.

When space big data involve the processing of personal data, the obligation to comply with the data protection principles mentioned in section 3.2.1 is required. Among the principles described in the GDPR, it is worth addressing the lawfulness of data processing, purpose limitation, and data minimisation, being the most relevant to space big data and closely connected to the rest of the principles mentioned in section 3.2.1.[81] As far as the lawfulness of data processing is concerned, several grounds can be deployed to justify it.[82] These include the consent of the data subject, the performance of a contract to which the data subject is a party, compliance with legal obligations, protection of vital interests, public interest and the exercise of an official authority, as well as the legitimate interests of the data controller.

For the purpose of the analysis in this thesis, the requirements of lawful data processing will be divided into two categories. The first one is the consent of the data subject. The second one includes the rest of the grounds, since they all relate to the purpose for which the data are processed. Regarding the consent of the data subject, the collection and processing of EO data falls under the freedom to use and explore outer space. In the case of location data and satellite-based internet traffic, the consent of the data subject is usually part of the terms and conditions that the data subject has accepted before using the device that collects and processes these data. Regarding the rest of the

81 Data accuracy and storage limitation depend on the purpose of the data processing, hence relate to purpose limitation. The principles of integrity and accountability are examined in association with other parts.

82 GDPR (n 52) art 6.

grounds for lawful data processing, since the purposes of collecting and processing space data are not defined in advance, the requirement is difficult to enforce and to monitor when enforced. The fact that such technology exists can be seen as contradictory to the requirement of lawful predefined purposes, given the unlimited options for its subsequent uses. To maintain the lawfulness of data processing, the controller can consider methods of encryption and pseudonymisation of data.

Likewise, as far as purpose limitation and data minimisation are concerned, predefining the purposes of data processing in the scope of space big data cannot easily find application in practice. Remote sensing imagery is collected and processed specifically because it can be used for any number of purposes, similar to satellite-enabled location data and internet connectivity. Since they all connect to the purposes of data processing, the requirements for lawful data processing, excluding consent, the purpose limitation, and the data minimisation will be examined together, as purpose-related requirements.

Given their role in compliance with the requirements for lawful processing of personal data, it is crucial to identify the data controller and the data processor at any given stage of the space big data lifecycle. Based on the aforementioned definition, the data controller can be the one that processes space big data at the stage of space big data processing. If that stage is followed by space big data analysis, the controller can be the one that determines the purpose and means of this analysis. If the processing and the analysis take place by different persons or entities, the title of the data controller may apply to all of them, depending on whether they remain involved in the lifecycle. Identifying the data controller at the stage of data collection and acquisition and the stage of data dissemination may be cumbersome, if that person or entity is only involved in that stage and does not determine the purpose and means of processing, such as a supplier of EO data or provider of space big data solutions. Arguably though, since the latter acquires or distributes these data to use or further disseminate them, they influence their processing. The same can apply to data storage, depending on whether it involves data processing. In the previous examples, the data controller may be joined by one or several data processors that should also comply with applicable data protection laws.

3.2.4 Preliminary conclusions on the privacy and data protection implications of space big data

Satellite technology enables the collection of large amounts of information about places and populations, as well as the location and movement of persons and vehicles. Furthermore, it enables internet connectivity and the transmission of information to various devices. These data collected and transmitted by

satellites are used in a great number of applications, including commercial and civil, as well as space and non-space-related applications.

Space big data eventually include personal data, namely information that identifies or is able to identify an individual. Privacy concerns are raised by high-resolution EO data and geolocation data, which may enable the identification and profiling of individuals, as well as the circulation of space-based internet connectivity data. However, they do not affect astronomy and other space-related data. Furthermore, the volume of data generated and disseminated by means of space technology, even when they do not amount to personal data, allows the deduction of identifiable information, either through combination with other available data or through complex data analytics. The connection between personal data and space big data gives rise to the application of data protection laws that establish obligations for those who collect and process personal information.

3.3 Intellectual property law

Intellectual property (IP) refers to the products of intellectual process and is protected by law through rights given to the producer or the owner of the intellectual product.[83] Intellectual property rights limit the use or distribution of an intellectual product, to safeguard the legitimate interests of the people and entities that are entitled to these rights. At the same time though, by enabling creators to secure their exclusive product, they further stimulate creation.[84] Space big data are produced, analysed, and used through various means of intellectual products, such as the databases that supply data used for data analysis and the methods deployed for making space big data and applications commercially viable.

This section examines the relevance of IP rights to space big data and explains the ways they can affect the space big data lifecycle. IP is governed by international rules and standards but is primarily regulated on a national level. Therefore, this section mainly focuses on the international provisions governing intellectual property rights, which provide for a minimum standard of protection. It also explains how the international framework is implemented in various jurisdictions, including in EU Member States, and other countries with dedicated regimes and significant presence in the field of space data, such as the US.

83 'What is intellectual property?' (*WIPO*) <https://www.wipo.int/about-ip/en/>.

84 Some general economic aspects of IP are discussed in R P Merges, 'Philosophical foundations of IP law: The law and economic paradigm' in B Depoorter, P Menell, D Schwartz (eds), *Research handbook on the economics of intellectual property law* (Research Handbooks in Law and Economics Series vol 1, Edward Elgar Publishing 2019) 72.

Section 3.3.1 describes the international, regional, and national IP framework, according to the different types of IP rights. On that basis, section 3.3.2 identifies the IP rights that are relevant to space big data, in terms of their collection, access, use, and dissemination.

3.3.1 The regulatory framework of intellectual property

Different types of intellectual property rights apply to different types of intellectual products and offer different levels of protection. The main categories of IP rights are copyrights, patents, trademarks, and trade secrets.[85]

A copyright is the right of a creator of an intellectual product over that product. A patent allows the exploitation of an invention upon the authorisation of its inventor and is granted by a competent national authority. A trademark is a sign that identifies and distinguishes the products of an enterprise and a trade secret protects confidential information with commercial value. This section focuses on the regulation of copyrights, patents, and trade secrets since space big data do not fall under the protection of trademarks.[86]

Intellectual property is regulated according to the jurisdiction at hand, according to international agreements. On the international level, the World Intellectual Property Organisation (WIPO) is a specialised UN agency that is tasked with the promotion and protection of IP rights worldwide.[87] It has developed and administers a set of international treaties that include provisions to protect and enforce IP rights and are internationally applicable. The provisions of these treaties are implemented in national laws, which determine how IP rights are treated within their jurisdiction. On the European level, the Treaty on the Functioning of the European Union provides for a level of harmonisation of IP rights. The EU Intellectual Property Office (EUIPO)[88] and the European Patent Office (EPO)[89] are in charge of the protection of IP rights, respectively trademarks and trade secrets, and patents. The European Observatory for Infringements of IPR[90] monitors the implementation of IP rights.

---

85 WIPO, *WIPO Intellectual Property Handbook* (WIPO Publications no 489 2004) 17, 40 and 68; 'Trade secrets' (*WIPO*) <https://www.wipo.int/tradesecrets/en/>.

86 Trademarks are not considered relevant to space big data, because they are meant to protect a brand or a product and not the information contained in the data. Some recommendations for extending the regulatory protection of trademarks to space activities can be found in C W Lackert, 'Trademarks in outer space: supporting the off-world economy' (*WIPO Magazine*, December 2021) <https://www.wipo.int/wipo_magazine/en/2021/04/article_0005.html>.

87 WIPO Convention (adopted 14 July 1967, entered into force 26 April 1970) 828 UNTS 3.

88 EU Intellectual Property Office <https://euipo.europa.eu/ohimportal/en/>.

89 European Patent Office <https://www.epo.org/index.html>.

90 EU Intellectual Property Office Observatory <https://euipo.europa.eu/ohimportal/en/web/observatory/home>.

– *Copyrights*

The Berne Convention for the Protection of Literary and Artistic Works[91] is the main international instrument regulating copyrights. Its provisions are complemented by the WIPO Copyright Treaty,[92] which along with the Berne Convention are the most widely accepted international agreements on copyright.[93] Other sources include similar provisions, such as the Universal Copyright Convention,[94] or are of more detailed scope, such as the TRIPS Agreement[95] of the World Trade Organization.

The main pillars of the regulation of copyrights are the creator's doctrine, the national treatment of copyright, and the automatic protection of copyrights. As far as the creator's doctrine is concerned, Article 2 of the Berne Convention protects literary and artistic works, regardless of their mode of expression. The main criterion is the creativity of the author, meaning the creator of the copyrighted work. Some non-exhaustive examples of creative work include photographic work, illustrations, maps, and work related to geography and topography. In this respect, copyright may extend to EO and GNSS data, which are based on or used for such forms of expression, but not to satellite-based connectivity data which include information that does not fit under the scope of copyrights.

Concerning the national treatment of copyrights, Article 5.1 of the Berne Convention provides that authors should enjoy the same rights in every contracting State as in their State of origin, whereas Article 5.3 provides that the protection of copyright in its State of origin is governed by national law. If the author is not a national of that State, they should enjoy the same rights as authors who are nationals. Consequently, although the protection of copyrights is geographically limited, in that they are only valid in the State in which they exist, contracting States should offer the same protection to nationals of other States.

---

91 Berne Convention for the Protection of Literary and Artistic Works (as amended) 1161 UNTS 3 (hereinafter Berne Convention).

92 WIPO Copyright Treaty (adopted 20 December 1996, entered into force 6 March 2002) 2186 UNTS 121 (hereinafter WIPO Copyright Treaty).

93 The Berne Convention has 181 Member States and the WIPO Copyright Treaty has 114 contracting parties. Status of the Berne Convention <https://www.wipo.int/export/sites/www/treaties/en/docs/pdf/berne.pdf>. Status of the WIPO Copyright Treaty <https://www.wipo.int/wipolex/en/treaties/ShowResults?search_what=C&treaty_id=16>.

94 UNESCO Universal Copyright Convention (as revised on 24 July 1971 and including Protocols 1 and 2) 828 UNTS 221. A thorough analysis of the Universal Copyright Convention can be found in J S Dubin, 'The Universal Copyright Convention' (1954) 42.1 California Law Review 89.

95 Agreement on Trade-Related Aspects of Intellectual Property Rights (15 April 1994) 1869 UNTS 299. An analysis of the copyright protection of the TRIPS Agreement can be found in C M Correa, *Trade related aspects of intellectual property rights: A commentary on the TRIPS Agreement* (2nd edn, OUP 2020) 107-141.

The automatic protection of copyrights refers to the lack of a registration requirement. According to Article 3.3 of the Berne Convention, a published work is one published with the consent of its author, without additional formalities. The Berne Convention provides for a minimum protection of copyrights. The national rules that transpose its provisions and the provisions of other international agreements may include higher standards.

The WIPO Copyright Treaty is a special agreement for extensive rights, according to Article 20 of the Berne Convention. Its provisions are similar to those of the Berne Convention in that it protects expressions, not ideas, procedures, or methods of operation.[96]The WIPO Copyright Treaty though extends the forms of protected expression. Article 4 of the Treaty includes computer programs among the protected literary work. This provision can give rise to copyright protection of computer programmes that are used for the processing and analysis of space big data, as well as computer programmes deployed for their generation and dissemination. Moreover, Article 5 includes databases, namely compilations of data, under the protected work. In that sense, compilations in any form are protected, as long as they are by selection or arrangement of content an intellectual creation. This provision protects databases as intellectual products and not the data they contain. Regardless, they can relate to databases of collected and processed space big data, placing them under copyright protection. A similar conclusion can be deducted from Article 11, under which the use of digitised data and information in which data are stored can be protected by their owner through technological means. Even though this does not create an IP right to protect these technological means as intellectual products, it allows digitised data and information to be better protected. Article 6 specifies that the exclusive right of authors means that their permission is required to make the intellectual product available or to transfer its ownership. The provisions of the WIPO Copyright Treaty should be implemented in its Member States via their national laws.[97]

Alongside the provisions of the Berne Convention and the WIPO Copyright Treaty, the EU has introduced a Directive specific to the protection of databases.[98] Its purpose is to extend copyright protection to databases, as their author's intellectual product, because of the selection or arrangement of their data, without protecting the data they include.[99] According to Article 1.1 of the Directive, any form of database is protected. Article 1.2 defines a database as a collection of independent works, data, or other material that is arranged systematically or methodically, that is accessible by electronic means. Computer

96 WIPO Copyright Treaty (n 92) art 2.
97 WIPO Copyright Treaty (n 92) art 14.
98 Directive 96/9/EC of the European Parliament and of the Council on the legal protection of databases [1996] OJ L 77/20 (hereinafter Database Directive). A similar protection, without specific rights regarding databases, can be offered through Berne Convention (n 91) art 2.5 and WIPO Copyright Treaty (n 92) art 5.
99 Database Directive (n 98) art 3.

programs that are used to compile or operate a database are not protected. Article 7 introduces a *sui generis* database right, which exists in parallel with potential copyright protection. In particular, Member States should provide for the right of the maker of the database, in a way that shows that there has been quantitative and/or qualitative investment, to obtain, verify, or present the contents of the database, in a way to prevent their extraction and re-utilisation. Under the Database Directive, databases are protected against temporary or permanent reproduction, translation, adaptation, arrangement, alternation, public distribution, display, and communication.[100] Other EU instruments on copyrights have not been sufficiently implemented by EU Member States.[101]

In the US, copyright is regulated by the Copyright Act.[102] Its protection covers original work fixed in a tangible medium of expression, from which this work can be perceived, reproduced or communicated, directly or with technical means.[103] Similar to the international framework, copyright protects the form and not the content of the expression.[104] These two criteria, the originality of work and the fixation in tangible form are the main requirements for establishing copyrights. The rights given to the owner of the copyright are the exclusivity to reproduce and distribute their work.[105] The exclusivity of copyright may be limited by the fair use of the copyrighted work.[106] Whether the use is fair depends on the nature and character of the use and the work, on the part of the copyrighted work that will be used, as well as on the effect of the use on the market for and value of the work.[107]

– *Patents*

Patents are regulated at the international level primarily through the Paris Convention for the Protection of Industrial Property,[108] which lays down rules for granting and registering patents. Patents grant exclusive rights to

100 Database Directive (n 98) art 5.

101 The EU copyright framework comprises of EU Directives and EU Regulations, as seen in <https://digital-strategy.ec.europa.eu/en/policies/copyright-legislation>. S Moan, 'Member States referred to the CJEU for failure to transpose copyright directives into national law' (*Kluwer Copyright Blog*, 15 March 2023) <https://copyrightblog.kluweriplaw.com/2023/03/15/member-states-referred-to-the-cjeu-for-failure-to-transpose-copyright-directives-into-national-law/>.

102 17 USC.

103 17 USC §102(a).

104 17 USC §102(b).

105 17 USC §106.

106 17 USC §107.

107 S Ayalp, 'Lost in space: The copyright dilemma' (2020) 7.2 American University Intellectual Property Brief 86, 97-98.

108 Paris Convention for the Protection of Industrial Property (as amended in 1979) 828 UNTS 305 (hereinafter Paris Convention).

inventors, namely the persons who have officially filed for the recognition of their invention.[109] Article 2 of the Paris Convention establishes the national treatment of patents as IP rights. In particular, inventors enjoy the same rights in other countries as the nationals of these countries. However, patents are valid within the jurisdiction under which they are granted. Should inventors file for a patent for the same invention in various jurisdictions, the patents will be independent of each other.[110] On the issue of jurisdiction, Article 5ter of the Paris Convention provides for an exception to the enforcement of patent rights. Specifically, it provides that vessels, aircraft, and land vehicles under the flag of a country, that pass through the jurisdiction of a different country, while carrying technology that could infringe patent protection in the country they pass, are not considered as infringing patent rights. This exclusion is solely applicable to the enforcement of patent rights and not to whether the technology at hand is patentable or patented or not.

Whether an invention can enjoy patent protection depends on domestic regulations, which describe the criteria for patentability. Therefore, unlike copyrights, there can be significant differences in the patent protection offered in various jurisdictions. For instance, the EU Patent Convention,[111] administered by the European Patent Office, establishes the conditions and procedures for granting European patents that can be requested in more than one contracting State.[112] Inventions in all technological fields can be patented, as long as they are inventive and susceptible to industrial application, except among others computer programs and mathematical methods.[113]

In the US, the Patent Act[114] includes rules for the patentability and protection of inventions. The criteria for granting a patent are its novelty and usefulness.[115] The US Patent Act also includes provisions regarding inventions in outer space.[116] Accordingly, inventions on a space object under US jurisdiction and control are considered as inventions within the US, unless otherwise arranged.

As far as the procedure for applying for and registering and patent is concerned, the WIPO Patent Cooperation Treaty[117] sets forth rules that simplify the patent filing system of the Paris Convention.

109 Paris Convention (n 108) art 4.
110 Paris Convention (n 108) art 4bis.
111 Convention on the Grant of European Patents (as amended) (hereinafter EU Patent Convention).
112 EU Patent Convention (n 111) art 3.
113 EU Patent Convention (n 111) art 52.
114 35 US Code.
115 35 US Code §101-103.
116 35 US Code §105. A similar provision is included in French Space Operations Act (2008) art 22.1.
117 WIPO Patent Cooperation Treaty (as amended in 2001).

Overall, patent protection safeguards exclusive rights and ideas. The kind of intellectual products that are protected depends on the jurisdiction at hand.

– *Trade secrets*

Trade secrets refer to confidential information that is privy to a closed group of people and that gives them a competitive advantage. The criteria that qualify a trade secret include its commercial value, its knowledge among a limited group of persons, and the reasonable steps that its holder takes to maintain its secrecy.[118] The premise of trade secrets' protection is that they are by definition treated confidentially. Once disclosed and if the disclosure is intentional, the secrets lose their protected status.[119] Trade secrets are not protected the same way as copyrights and patents, although they receive increasing recognition in legislation. In practice, the violation of a trade secret constitutes an unfair practice. Nevertheless, regulations are in place in the EU and the US to define what trade secrets are and how they can be protected.

In the EU, trade secrets are the subject of the Directive of Trade Secrets.[120] According to its provisions, a trade secret can be lawfully acquired, used, or disclosed under certain circumstances,[121] generally when honest commercial practices are followed. Consequently, a trade secret is lawfully transferred when it is the result of an independent discovery or creation, when it is the outcome of the examination of a product or object that is publicly available or lawfully possessed, or when employees act under workers' rights. On the contrary, the acquisition, use, and disclosure of trade secrets are unlawful when they take place without the consent of the trade secret holder and specific conditions are in place.[122] In particular, unauthorised access, appropriation or copying contribute to the unlawful transfer of trade secrets. Likewise, people who have unlawfully acquired trade secrets, breach confidentiality agreements or other contractual duties infringe trade secrets. The Directive also provides for the adoption by Member States of precautionary measures and necessary safeguards to protect the interests of trade secret holders.[123]

118 'Trade secrets' (*WIPO*) <https://www.wipo.int/tradesecrets/en/tradesecrets_faqs.html>, M Risch, 'Why do we have trade secrets' (2007) 11 Marquette Intellectual Property Law Review 1, 6-8.

119 J C Steidman, 'Trade secrets' (1962) 23 Ohio State Law Journal 4, 5-9.

120 Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition [2016] OJ L 157/1 (hereinafter EU Directive on Trade Secrets).

121 EU Directive on Trade Secrets (n 120) art 3.

122 EU Directive on Trade Secrets (n 120) art 4.

123 The EU Intellectual Property Office compiled in 2018 a Baseline of Trade Secret Litigation in the EU Member States <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2018_Baseline_of_Trade_Secrets_Litigations_in_EU_Member_States/2018_Baseline_of_Trade_Secrets_Litigations_in_EU_Member_States_EN.pdf>.

In the US, trade secrets fall under the scope of the Defend Trade Secrets Act of 2016.[124] The Act describes the measures in place to protect the rights of a trade secret holder, including defending the misappropriation of the secret in court and benefiting from legal remedies. On the level of States, the Uniform Trade Secrets Act[125] provides specific requirements for the protection of trade secrets and the procedures that can be taken against their misappropriation.

3.3.2 Intellectual property in the scope of space big data

IP rights are relevant to the space sector because it is characterised by the use of sophisticated technology, which is in principle protected by IP and offers competitive advantages to its owners and creators.[126] Particularly in the context of space big data, IP rights affect the use and dissemination of data, which may be limited or conditional. IP rights are mostly relevant to the part of data processing and analysis, which can be considered an intellectual creation. They can also relate to databases that are protected as creations, as well as to trade secrets involved in the space big data lifecycle. Therefore, the processing and distribution of space data included in space big data may be impacted by copyrights, patents, or trade secrets that protect related information, know-how, and technology.

– *Copyright in space data and databases*

Copyrights protect the expression or the creative representation of an idea, but not the idea as such.[127] Applied to the space big data lifecycle, copyrights relate to the processing and analysis of space data, as a form of intellectual work, but not to the information contained therein. As was mentioned in section 2.1.2, space data in their raw form undergo preliminary processing, in order to become usable, whereas space data processed in various levels are further developed into analytical results. In these instances, if the copyright requirements of the applicable laws are fulfilled, how space data are presented, used, and distributed may be exclusive or limited, based on the conditions set forth by the owner of the IP right.

Whether space data are protected through copyright depends on the level of creativity involved in their processing and on whether the outcome of this procedure can be protected. In principle, as explained in section 2.1.3, space

124 Defend Trade Secrets Act of 2016.

125 Uniform Trade Secrets Act (Uniform Law Commission, 1985).

126 A M Balsano, 'Intellectual property rights and space activities' (*ESA Bulletin 79*, August 1994) <https://www.esa.int/esapub/bulletin/bullet79/balsano.htm>.

127 R Oosterlinck, 'Legal protection of remote sensing data' in *Proceedings of the twenty-seventh Colloquium on the Law of Outer Space* (AIAA 1985) 115.

data can be processed for any number of uses, based on the desired purpose. Nominal processing may not be protected, as the creative expression involved is limited.[128] In such cases, the creator may need to engage in further processing or value-added applications, to enjoy copyright protection and maintain control over the data. On the other hand, analytical processing requires complex knowledge that may fall under copyright. Therefore, the use of space data can determine whether the process of making space data usable in a given context will be protected through copyright. Separately, the software that is used for data processing could be considered as the tool to express an idea, hence potentially protected by copyright. However, this is not in the scope of the copyright regulations explained in section 3.3.1 but may be treated differently in various national laws.

The conditions under which copyrighted space data can be used are determined by the creator and can vary among them. Licenses and other forms of user agreement for space data dictate who and how can use them. These agreements serve as protection of the IP rights of the creator. However, they can also function independently from the presence of IP rights, as a way for the data owner to control their data, regardless of their legal status as creator, to control their data.[129] One of the ways that are used to protect copyrighted space data is the watermarking of EO data. Watermarks constitute visible and invisible marks on EO images that verify the authenticity of copyrighted images.[130] Open access space data do not have significant restrictions as far as copyright is concerned.

Some copyright laws extend their scope to databases, as forms of intellectual creations or *sui generis* intellectual products. In that case, databases that contain space data may be protected. The protection of databases is mostly relevant to EO data since satellite-enabled location data and space-based connectivity data are in principle not stored in databases. The degree to which a database is a creative work and should be the subject of protection is unclear in the laws described in section 3.3.1 and depends on the case at hand. The question of whether the compilation of matrixes that make up a satellite image can be justified as a database is a theoretical one, as the relevant regulations

128 J R West, 'Copyright protection for data obtained by remote sensing: How the data enhancement industry will ensure access for developing countries' (1990) 11 Northwestern Journal of International Law and Business 403, 410.

129 P A Salin, 'Proprietary aspects of commercial remote-sensing imagery' (1992) 13.2 Northwester Journal of Internal Law and Business 349, 365-371.

130 More about the process of digital watermarking of satellite images and its use for copyright protection can be found in P H Hsu, C C Chen, 'Feature-based digital watermarking for remote sensing images' (2012) XXXXIX-B3 International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences <https://www.int-arch-photogramm-remote-sens-spatial-inf-sci.net/XXXIX-B3/473/2012/> 474; G Yuan, Q Hao, 'Digital watermaking secure scheme for remote sensing image protection' (2020), 17.4 China Communication 88, 88-90.

provide for the collection of independent data for the compilation of a database.[131]

– *Patents in technology for space data analysis*

Patents grant exclusive rights to inventors, namely the persons who have officially filed for the recognition of their invention.[132] In the framework of space big data, patents can be divided into two instances, inventions that take place in outer space and inventions that take place on Earth and relate to space data.

As far as inventions in outer space are concerned, patents apply to technology and objects under a State's jurisdiction. If a space object is registered by a State and hence placed under its jurisdiction,[133] an invention on board of that object could be protected under the laws of the State of registry.[134] A dedicated regime for IP on board the International Space Station (ISS) is established by the ISS Intergovernmental Agreement (IGA), which governs the cooperation of the ISS partners. Each of the partners provides an element of the ISS, as described in the Annex of the IGA. According to Article 5 of the IGA, each partner retains jurisdiction and control over the element of the ISS under its registry.[135] Consequently, for the purpose of IP protection, an activity on the ISS is considered to have taken place on the territory of the partner State that has registered the respective ISS element.[136] In addition, the Paris Convention clarifies that vessels, aircraft, and land vehicles under the flag of a State do not violate patent protection, if they carry items that may infringe patent laws in the jurisdiction through which they are passing. This provision refers to the enforcement of patent protection and not to the ability of an item to be patented. Accordingly, it could be supported that a space object registered in a State falls under this provision. However, spacecraft are

131 M Mejia-Kaiser, 'Satellite remote sensing data in databases' (1997) 22 Annals of Air and Space Law 495, 499-500.

132 Paris Convention (n 108) art 4.

133 By the means of Article VIII OST, which confers jurisdiction and control to the launching State that registers a space object, as explained in section 3.1.3.

134 H Dunlop, 'Are satellites beyond the reach of patents?' (*Maucher Jenkins*, 18 January 2022) <https://www.maucherjenkins.com/commentary/are-satellites-beyond-the-reach-of-patents>.

135 The ISS elements provided by ESA are registered by ESA, as agreed by the ESA Member States that participate to the ISS.

136 Intergovernmental Agreement on Space Station Cooperation (signed 29 January 1998, entered into force 20 February 2008) [2008] ATS 19 art 21.1. A concise analysis of the IP provisions in the Agreement can be found in R Moenter, 'The International Space Station: Legal framework and current status' (1999) 64.4 Journal of Air Law and Commerce 1033, 1052-1054; A M Balsano, J Wheeler, 'The IGA and ESA: Protecting intellectual property rights in the context of ISS activities' in F G von der Dunk, M M T A Brus (eds), *The International Space Station* Martinus Nijhoff, 2006) 63-78.

not considered among the vessels mentioned in the Paris Convention, therefore the exception does not apply to them.[137]

Most of the patented technology that is relevant to space data does not concern inventions in space, but the use of inventions on Earth. In this regard, novel technologies that are used for handling and processing space data can be protected as patents. Especially the private entities that provide services that use data for various purposes, rely on proprietary software, which, combined with their expertise in processing and analytics, offers competitive advantages.[138] Patents involved in value-added products and applications are among the most common types of patents in the space sector value chain.[139]

– *Trade secrets in the space big data lifecycle*

Trade secrets can be found in several stages of the space big data lifecycle. Since they are not registered and the main premise of their legal protection is the effort to keep them confidential, it is difficult to estimate their presence and impact. One of the main elements of trade secrets is their commercial value. Therefore, given the growing privatisation and commercialisation in the field of space data, the deployment of trade secrets can be safely assumed for EO data, GNSS data, and satellite-based internet data. For instance, the collection of EO data, the tailored analysis of space data, and the marketing of space data applications can involve trade secrets, held by companies with technical capabilities and market needs. Trade secrets can also be used as a means to protect space data and the value added to them that cannot be protected through copyrights and patents given their specific requirements.[140] Conversely, the question of whether EO data can be used to expose trade

137 'Intellectual property and space activities' (Issue paper prepared by the International Bureau of WIPO, April 2004) <https://www.wipo.int/export/sites/www/patent-law/en/developments/pdf/ip_space.pdf> 20.

138 H Ludwig Moeller, 'EO open data in Europe – Intellectual property and services market in China and the U.S., ESPI Perspectives February 2023' (*ESPI*, 6 March 2023) <https://www.espi.or.at/news/february-2023-directors-perspective/>.

139 E Collette, D Haight, S Martineau, M Neville, A Parsons, 'Patents in space – Highlighting innovation in the Canadian Space Sector' (*Canadian Intellectual Property Office and Canadian Space Agency*, 2018) <https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/vwapj/CIPO-Patents-in-Space-Report_e.pdf> 24. Indicative numbers, such as the fluctuating numbers of space-related patents and the space domains they relate to can be found in 'The space economy at a glance' (*OECD*, 2014) <https://read.oecd-ilibrary.org/economics/the-space-economy-at-a-glance-2014_9789264217294-en> 69.

140 The role of trade secrets, compared to patents and other IP rights, is discussed in D L Burk, 'Protection of trade secrets in outer space activity: A study in federal preemption' (1993) 23.2 Seton Hall Law Review 560, 589-593.

secrets by revealing information that is otherwise unavailable has been presented.[141]

3.3.3 Preliminary conclusions on the intellectual property implications of space big data

Space big data rely on the intellectual processes that are protected through IP rights for rendering usable and informative applications. The processing, use, and distribution that add value to space data can be limited or conditioned by copyright or patent restrictions, whereas parts of the space big data lifecycle may be covered by trade secrets. *Copyrights* limit the creative process involved in turning raw data into processed data and analysed information, which are subject to the conditions set forth by their creator or owner. *Patents* grant exclusive rights to the inventors of novel technologies and methods that are used in the collection and processing of space data. *Trade secrets* are used to withhold information with commercial value that offers a competitive advantage to those privy to them.

Even though intellectual property rights are valid and regulated within the jurisdiction in which they are granted, there are common characteristics among the various frameworks. Copyrights depend mainly on the creativity of the intellectual work, patents require novelty, and trade secrets require the conscious confidentiality of commercially valuable information. The IP rights that are most closely related to space big data are copyrights, which protect creative intellectual work and, conditionally, databases. Copyrights can be linked to EO data that are pre-processed, processed, analysed, and disseminated, especially on a commercial level. EO data from open-access sources may also come with minimal copyright restrictions. Satellite-enabled location data do not usually relate to copyrights, since they are provided by publicly-funded GNSS missions that do not impose restrictions on that basis. Space-based connectivity data do not fall under the categories that are protected by IP laws, since they are not commonly collected in databases and do not involve creative processing. Astronomy data and other data related to space may be protected as database collection or when they involve creative intellectual work. Besides copyrights, technologies, and tools used to handle the different types of space data may be protected by patents and trade secrets.

141 C M Gayton, 'Commercial satellite imagery: CI, KM, and trade secret law' (2007) 37.2 VINE: The Journal Of Information And Knowledge Management Systems 192.

3.4 Cybersecurity law[142]

The cyber dimension is embedded in a considerable part of space activities, thus the issue of cybersecurity becomes relevant to satellites, as well as to the data they generate, carry, and transmit.[143] Cyber risks are a factor of growing concern, given the increasing reliance of space systems on network services, as well as the growth in the field of space applications available to various users.[144] In the framework of space activities, cyber risks can consist of interference with satellite signal transmission and interference with stored data.[145] Whereas both risks can result in serious harm, damage to stored data is more easily identifiable, while signal transmission is a temporary occurrence, which is also regulated by means outside the scope of cyber regulations.[146] Therefore, this section focuses primarily on unauthorised access to space data on the ground and in outer space but also addresses the transmission of space data to and from satellites. Its purpose is to address the existing regulatory framework regarding cybersecurity vis-à-vis the flow and volume of information needed in the framework of space big data.

Section 3.4.1 elaborates on the EU cybersecurity regime, to determine its applicability to space big data through its connection to current methods of space data transmission and storage. It also attempts to define cybersecurity in space activities and space big data by emphasising the notions of information systems and cyber threats within the structure of space big data systems. Section 3.4.2 analyses cybersecurity in the context of space big data, by reference to cyber threats against stored and traffic data.

142 Section 3.4 is based on a paper presentation during the International Astronautical Congress in 2018, which was published as D Stefoudi, 'The relevance and applicability of cybersecurity laws with regard to data storage on board satellites and on the ground' (2019) 4/5 ASL 425.

143 L Martinez, 'The legal dimensions of cyber-conflict with regard to large satellite infrastructures and constellations' in P J Blount, T Masson-Zwaan, R Moro-Aguilar, K U Schrogl (eds), *Proceedings of the International Institute of Space Law 2016* (Eleven International Publishing 2017) 431-443.

144 'Thrip: Espionage group hits satellite, telecoms, and defense companies' (*Symantec*, 19 June 2018) <https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets>; D Werner, 'Satellite communications firms remain vigilant as cyber threats evolve (*Space News,* 20 February 2018) <https://spacenews.com/satellite-communications-firms-remain-vigilant-as- threats-to-their-satellites-networks-evolve/>; M Holmes, 'Cyber experts: The truth about the threats to satellite' (*Via Satellite,* 15 May 2017) <https://interactive.satellitetoday.com/cyber-experts-the-truth-about-the-threats-to-satellite/>.

145 S Kaiser, M Mejia-Kaiser, 'Cyber security in air and space law' (2015) 64 ZLW 396, 404.

146 Namely by the International Telecommunication Union framework. M Sakamoto, 'ITU and harmful interference prevention' in M Hofmann, *Legal rules for interference-free radio communication: 3rd Luxembourg workshop on space and satellite communication law* (Nomos/Hart 2015) 89.

3.4.1 The EU regulatory framework on cybersecurity

Cybersecurity is commonly understood as the protection of electronic systems against external threats and the measures taken in this regard.[147] The term is surrounded by ambiguity and is often used interchangeably with or by association with other terms, such as cyber operation, cyberattack, or cyber warfare.[148] The notion appears with similar characteristics in various texts, but there is no one agreed definition.[149] For example, the International Standardisation Organisation (ISO) defines cybersecurity as the 'preservation of confidentiality, integrity, and availability of information in the cyberspace'.[150] The ITU describes cybersecurity as the collection of measures 'that can be used to protect the cyber environment and organisation and user's assets'.[151] Cybersecurity can be also understood by reference to its antonyms, cyber threats, and cybercrimes, which describe situations where security is of the essence. In principle, the term 'cybersecurity' refers to the protection of cyberspace, the intangible dimension consisting of networks that store and transfer digital information of all sorts.[152] Cybersecurity law, being currently under development, is of limited content and scope. There are international, regional, and national initiatives to regulate cyber activities, but they lack

147 'Cybersecurity' (*Merriam Webster)* <https://www.merriam-webster.com/dictionary/cyber security>; 'Cybersecurity' (*Cambridge Dictionary*) <https://dictionary.cambridge.org/dictionary/english/cybersecurity>; Gartner defines cybersecurity as the combination of people, policies, processes and technologies employed by an enterprise to protect its cyber assets. 'Cybersecurity' (*Gartner*) <https://www.gartner.com/en/information-technology/glossary/cybersecurity>. IBM describes it as the practice of protecting critical systems and sensitive information from digital attacks. 'What is cybersecurity?' (*IBM*) <https://www.ibm.com/topics/cybersecurity>. A concise definition is provided by NATOTerm that describes cyber security as 'the application of security measures for the protection of communication, information and other electronic systems, as well as the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation. 'Cyber security' (Record 39183, *NATOTerm*) <https://nso.nato.int/natoterm/Web.mvc>.

148 J Kulesza, R Balleste (eds), *Cybersecurity and human rights in the age of cybersurveillance* (Rowman and Littlefield Publishers 2015) 1–4; T Topina, C Callanan, *Self- and co- regulation in cybercrime, cybersecurity and national security* (Springer Briefs in Cybersersecurity, Springer 2015) 5.

149 The term cybersecurity is used differently by various stakeholders. A representation of various definitions by -among others- NATO, ITU, and ISO can be found in 'Definition of cybersecurity – Gaps and overlaps in standardisation' (*ENISA*, July 2016) <https://www.enisa.europa.eu/publications/definition-of-cybersecurity>, 19.

150 Cybersecurity is also phrased as 'cyberspace security'. ISO/IEC 27032:2012, Information technology-Security techniques-Guidelines for cybersecurity, par. 4.20.

151 Recommendation ITU-T X. 1205, Series X: Data networks, open system communications and security – Telecommunication security – Overview of cybersecurity (ITU 2018) 6.

152 R A Wessel, 'Towards EU cybersecurity law: Regulating a new policy field' in N Tsagourias, R Buchan (eds), *Research handbook on international law and cyberspace* (1st edn, Research Handbooks in International Law Series, Edward Elgar Publishing 2015) 407–408.

uniformity, since they introduce different definitions, address different types of cyber operations, and have different scopes of application.

Whereas cybersecurity regulations are designed to safeguard the integrity of data systems from external tampering, their relevance and applicability to space operations, particularly space big data, has not been established.

Cybersecurity is regulated on various levels, including regional and national laws. This section examines the cybersecurity framework in the European Union as established by the EU NIS 2 Directive[153] and refers to the framework of the US, given its significant presence in the space sector. In particular, this section elaborates on the EU NIS 2 Directive and occasionally makes comparisons with the US Cybersecurity Act, the US National Cybersecurity Strategy, and the US Internet of Things Cybersecurity Act. These documents constitute some recent legislative examples and regulate cybersecurity on different levels and to a different extent. Their common denominator is the explicit reference to the issue of security, whether this is mentioned as cybersecurity, security of NIS, or other equivalent terms. The following sections analyse the scope of the EU cybersecurity framework, its subjects, and its obligations. They also elaborate on the cybersecurity frameworks of the US.

– *The scope of protection of the EU cybersecurity framework*

Cybersecurity in the European Union is regulated by the Directive on Network and Information Systems, also known as the NIS 2 Directive. The EU NIS 2 Directive, adopted in 2022, repeals the previous EU NIS Directive, adopted in 2016, and provides more comprehensive cybersecurity provisions that also apply to parts of the space sector. The NIS 2 Directive is binding upon all EU Member States and calls for the implementation of national strategies that ensure a minimum level of cybersecurity. The Directive recognises in its preamble that existing capabilities to protect NIS against cyber threats are not sufficient, since each Member State is differently prepared to tackle and mitigate them.[26] Therefore, it aims at setting a common minimum level of security through national cybersecurity strategies, cooperation on the level of EU and the level of EU Member States, as well as cybersecurity risk-management and reporting obligations. Towards this end, it imposes the obligation to the States to regulate the conduct of operators of certain categories of essential and

153 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1 (hereinafter EU NIS 1 Directive). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333/80 (hereinafter EU NIS 2 Directive).

important entities, in a way that would comply with a minimum level of cybersecurity.

Cybersecurity is defined in the NIS 2 Directive as the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.[154] Networks and information systems (NIS) are defined as electronic communication networks and devices or groups of interconnected or related devices, one or more of which perform automatic data processing. The definition also includes the digital data stored, processed, retrieved, and transmitted. Electronic communications refer to transmission systems and other resources that permit the conveyance of signals, explicitly mentioning satellite networks among them.[155] Consequently, within the scope of the Directive, NIS include satellite systems and ground infrastructure, along with the transmitted and stored data.

– *The subjects of the EU cybersecurity framework*

Under the NIS 2 Directive, the obligation to achieve a sufficient level of security for network and information systems is vested upon operators of essential and important entities.[156] Essential entities are the enterprises of Annex I of the Directive that exceed medium-size qualifications,[157] thus enterprises that employ more than 250 persons and have annual turnover exceeding € 50 million, and/or an annual balance sheet exceeding € 43 million.[158] Annex I explicitly mentions the space sector as one of the types of essential enterprises that fall under the scope of the Directive. In particular, it refers to 'operators of ground-based infrastructure, that is owned, managed, and operated by Member States or by private parties, that support the provision of space-based services, excluding the providers of public electronic communication services'. In this regard, NIS in the ground-based segment of the space big data lifecycle are protected according to the Directive, when offered by larger entities. Essential are also the entities of the sectors mentioned in Annex I and II that are identified by the Member States as essential.[159] Member States may

154 The definition is found in Regulation (EU) 2019/881 of the European Parliament and of the Council of April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L 151/15 art 2.1, according to EU NIS 2 Directive (n 153) art 6.2.

155 EU NIS 2 Directive (n 153) art 6.1 (a), referencing Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36 art 2.1.

156 EU NIS 2 Directive (n 153) art 3.

157 EU NIS 2 Directive (n 153) art 3.1(a).

158 The definition of micro, small and medium-sized enterprises can be found in Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises 2003/361/EC [2003] OJ L 124/36 annex art 2.1.

159 EU NIS 2 Directive (n 153) art 3.1(f).

qualify such services as essential if they are the sole provider in that State of a service essential for the maintenance of critical societal or economic activities if their disruption could have a significant impact on public safety, security, and health if their disruption could induce a significant systemic risk, and if they have specific importance in their respective sector.[160] Annex I refers to the space sector, which could be identified by a Member State as essential, and could hence cover the ground segment of small and medium entities that fulfil the said conditions. Furthermore, essential services are qualified trust service providers, top-level domain name registries, service providers of Domain Name Services, providers of public electronic communication networks or publicly available electronic communication services larger than medium-sized, public administration entities,[161] and entities that Member States identify as essential.[162] Parts of the space big data lifecycle may be offered in the framework of such services, and therefore can fall under the scope of the Directive.

The entities mentioned in Annex I that do not qualify as essential due to their small or medium size, are considered important entities.[163] Therefore, the NIS of the ground segment of small and medium entities of the space sector, which is included in Annex I, fall under the scope of the Directive.

Whereas several parts of the space big data lifecycle may fall under essential or important entities, it is only essential entities that have to comply by default with the protective measures of the NIS 2 Directive.[164] Important entities, on the other hand, are supervised *ex post* as to whether they adhere to these measures, in case cyber incidents occur.[165]

– *Obligations under the EU cybersecurity framework*

To provide minimum harmonisation, the Directive calls for EU Member States to establish a national cybersecurity strategy for NIS under the scope of the Directive.[166] The strategy should include strategic objectives, resources for achieving them, as well as policy and regulatory measures for implementing them. In particular, it should provide for a governance framework, the identification of the relevant assets, risk assessment, as well as measures for prepared-

160 EU NIS 2 Directive (n 153) art 2.2(b) to 2.2(f).
161 Central government according to the national law of Member States, EU NIS 2 Directive (n 153) art 2.2(f)(i).
162 Member States can identify entities as essential according to their national law or to EU NIS 1 Directive (n 153).
163 EU NIS 2 Directive (n 153) art 3.2.
164 EU NIS 2 Directive (n 153) art 32.
165 EU NIS 2 Directive (n 153) art 33.
166 EU NIS 2 Directive (n 153) art 7.1.

ness, responsiveness, and recovery from incidents.[167] The policy should also involve cybersecurity in the supply chain for ICT products, and cybersecurity-related requirements for ICT products, among other measures. Member States should ensure that the entities under the scope of the Directive implement cybersecurity risk-management measures.[168] These measures should entail risk analysis, incident handling, business continuity, supply chain security, assessment of the effectiveness of measures, training, cryptography, and encryption methods, as well as multi-factor or continuous authentication.[169]

Furthermore, EU Member States should designate authorities competent for monitoring the application of the Directive and single points of contact for matters regarding NIS security and cooperation with other Member States in this field.[170] Measures concerning national and EU-wide cooperation in exchanging information and improving the level of cybersecurity across EU Member States are also envisioned in the Directive.

The EU NIS 2 Directive has a much broader scope than the NIS Directive, in that it covers NIS of the ground infrastructure involved in space big data, either as essential or as important services. Annex I refers to ground infrastructure that supports the provision of space-based services and the definition of the NIS that are protected includes satellite communications, such as satellite signals. Therefore, the space infrastructure is also covered by the Directive, as part of the provision of space-based services and as part of the NIS governed by the Directive.

– *The US cybersecurity framework*

In the US, cybersecurity is not regulated centrally. Each State has its own cybersecurity-related legislation, whereas, on a federal level, most regulations address specific sectors, such as healthcare and financial services.[171] The Cybersecurity Act of 2015, the Internet of Things Cybersecurity Improvement Act of 2017 (IoT Act), the Memorandum on Space Policy Directive-5 Cybersecurity Principles for Space Systems, and the National Cybersecurity Strategy include more general cybersecurity provisions. Their scope varies and can be interpreted to apply to parts of the space big data lifecycle.

The National Cybersecurity Strategy of 2023[172] brings two shifts in the way cybersecurity is treated in the US framework. First, it places the burden

167 According to EU NIS 2 Directive (n 153) art 6.6, an incident is an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

168 EU NIS 2 Directive (n 153) art 21.1.

169 EU NIS 2 Directive (n 153) art 21.2.

170 EU NIS 2 Directive (n 153) art 8.

171 Cybersecurity Act of 2015 (hereinafter Cybersecurity Act), Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act of 1999.

172 National Cybersecurity Strategy of March 2023.

of maintaining cybersecurity from the smaller actors to larger organisations that are best positioned to reduce risks for a wider range of entities. Second, it promotes resilience as a long-term investment. It also introduces a five-pillar approach to cybersecurity, including the defence of critical infrastructure, the disruption of threat actors, a security and resilient-driven market, investments in resilience, and international partnerships.

The Cybersecurity Act defines cybersecurity as the security, availability, confidentiality, and integrity of information systems or information that is stored on, processed by, or transiting an information system against threats and vulnerabilities.[173] An information system is defined as a discrete set of information resources organised to collect, process, maintain, use, share, disseminate, or dispose of information.[174] Such a broad definition could encompass satellite systems that collect and disseminate information, as well as their corresponding ground segments. When it comes to the IoT Act, the definition of information systems is limited to IoT devices purchased by the federal government, namely the devices with the capability of connecting to the internet and being regularly connected thereto.[175] These devices are physical objects with computer processing capabilities that can collect, send, and receive data, The Act does not clarify the meaning of regular connection to the internet, a requirement that might narrow down the wide variety of internet-connected devices. As previously mentioned, satellites are not only part of the Internet of Things but also provide internet connectivity. In this sense, they could fall under the devices protected by the Act, especially since they generate and transmit data. Likewise, ground station facilities, provided they maintain a regular connection to the internet, might be included under this definition.

The Memorandum on Space Policy Directive -5 focusing on Cybersecurity Principles for Space Systems[176] is specifically designed to address cybersecurity in space activities. It directs to governmental entities to design and implement cybersecurity measures for space systems.[177] Its provisions include a broad definition of space systems encompassing both ground and space networks and their connecting user or mission network, hence providing broad coverage of satellite systems. The Directive highlights the contribution of space systems to national critical infrastructure and the importance of preserving

173 Cybersecurity Act (n 171) sec 102.4 and 102.5. Similar is the definition of cybersecurity in the Internet of Things Cybersecurity Improvement Act of 2020 sec 2.10 (hereinafter IoT Act).

174 44 USC §3502.

175 IoT Act (n 173) sec 2.6.

176 Memorandum on Space Policy Directive-5 – Cybersecurity Principles for Space Systems (2020) (hereinafter Space Policy Directive-5).

177 M Young 'How does Space Policy Directive-5 change cybersecurity principles for space systems?' (*Aerospace Corporation*, 14 September 2020) <https://aerospace.csis.org/how-does-space-policy-directive-5-change-cybersecurity-principles-for-space-systems/>.

their reliability and efficiency.[178] It provides for a comprehensive scope of protection of space systems against cyber threats and calls for specific methods to be followed by the operators and owners of space systems. The definition of space systems encompasses all aspects of space operations, including space networks, ground networks, and mission and use networks.

As far as the level of protection of the US cybersecurity framework is concerned, the Cybersecurity Act provides for the sharing on behalf of the federal government of information regarding cyber threat indicators with the entities concerned,[179] and the authorisation for preventing, detecting, analysing, and mitigating threats.[180] The Act includes several types of threats that could be indicated through the sharing of information, including malicious reconnaissance, defeating a security control or exploitation of vulnerabilities, security vulnerabilities, malicious cyber command, and control, as well as any combination of the above and any harm caused therefrom.[181] The Act also describes methods in which information about threats should be communicated to the federal government and ways in which defence measures against cyber threats can be launched.[182] The Act could find application to the case of space systems collecting and transmitting data, as well as to the ground stations where space big data is stored. However, it does not set up specific cybersecurity standards that should be followed by the operators of such systems nor does it establish enforcement provisions. Combined with the fact that the notification and information exchange framework of the IoT Act is voluntary and does not create a duty to share,[183] its protective scope is of limited significance. The IoT Act requires inserting specific clauses into the purchase contracts that US Government entities conclude with third parties,[184] whereby the vendors agree to meet the prescribed standards. Even though these standards are not spelled out explicitly, reference is made to known vulnerabilities and notification about system deficiencies.[185] The potential contractors are required to disclose in advance any vulnerabilities of the IoT devices they are providing, to ensure that any update on the devices' software is performed in a secure manner,[186] as well as to refrain from retaining credentials that allow them to remotely access or operate these devices.[187] This requirement on behalf of the contractor not to withhold credentials that

178 Space Policy Directive-5 (n 176) sec 1.
179 Space Policy Directive-5 (n 176) sec 3.
180 Space Policy Directive-5 (n 176) sec 4.
181 J L Tran, 'Navigating the Cybersecurity Act of 2015' (2016) 19 Chapman Law Review 483, 487-488 and 495-497.
182 Space Policy Directive-5 (n 176) sec 5.
183 P Eddington, 'OPM, CISA, and the cybersecurity oxymoron' (*Just Security*, 2 July 2015) <https://www.justsecurity.org/24360/opm-cisa-cybersecurityoxymoron>.
184 IoT Act (n 173) sec 3a, US IoT Act.
185 IoT Act (n 173) sec 3a.1A.i par I.
186 IoT Act (n 173) sec 3a.1A.i par II.
187 IoT Act (n 173) sec 3a.1A.i par IV.

allow the remote operation of the IoT device might prove challenging considering the operation of satellite systems. Even though the protection of satellite and space big data systems remains outside the main purpose of the IoT Act, it is worth noting that it fails to recognise the reliance of IoT devices on space technology and the information, in the form of data, circulated through satellite systems.

Space Policy Directive-5 focuses on improving the cybersecurity of space systems in the US by laying down principles specific to the protection of space-based and ground-based assets and calling for cooperation among relevant stakeholders. The principles comprise measures of protection against cyber threats along with recommendations for cooperation and exchange of information. As far as cyber threats are concerned, Principle (a) refers to cyber activities that could manipulate, deny, degrade, disrupt, destroy, surveil, or eavesdrop on space systems, hence addressing a broad range of cyber threats that could affect the proper operation of space systems. To secure against these threats, Principle (a) calls for their continuous monitoring and anticipation, as well as for adaptation to mitigate them. At the same time, the owners and operators of space systems should ensure that they can retain positive control over space systems,[188] which will receive timely and orderly authorised commands.[189] To this end, certain mechanisms are suggested including protection of space systems against unauthorised access, elimination of physical vulnerabilities, protection against jamming and spoofing, protection of ground systems, and management of supply chain risks. The Directive also invites the implementation of the said principles through official channels and the development of best practices among the owners and operators of space systems.

3.4.2 Cybersecurity in the scope of space big data

In order to understand the connection between space big data and cyber technology, and subsequently also the challenges from their interdependence, it is essential to contextualise the basic terms, namely cyber operations, and cybersecurity, in the framework of space big data. These notions are examined taking into account the preceding definitions, as well as the particular features of the space data lifecycle, from the point of data collection until the distribution of the final data product. The following sections focus on the cyber element of space activities, the cyber element of space big data, and explain the cyber threats against space big data.

188 Space Policy Directive-5 (n 176) princ (b).
189 Space Policy Directive-5 (n 176) sec 2 (c).

– *The cyber element of space activities*

'Cyber' is an adjective used to attach to its adjacent terms the meaning of being connected to some sort of digital network.[190] Despite the lack of an internationally agreed definition, the term is deployed to describe an immaterial dimension of the information technology networks[191] and is often used interchangeably with the term 'internet connection'.[192] Initially, cyber law documents were restricted to computer networks,[193] but they have developed to include the broader notion of network and information systems (NIS).[194] The cyber element is an enabler as well as a part of every modern technology that involves remote communication, including space technologies and applications. In the framework of the latter, cyber is present in any system that is based on or involves the use of a network. In the case of space big data, this network incorporates the transmission between a satellite and a ground station or between satellites, as well as the access to data stored on the ground and onboard space objects.[195]

The increasing reliance on satellite systems for telecommunication, network connectivity, and remote sensing has extended cyberspace to more space-related devices and systems. With the advancement of space technology and space applications, a simple transmission between a satellite and a ground station has evolved to satellites enabling or being part of the ultimate cyber infrastructure, the Internet of Things.[196] For the purposes of this analysis,

190 P W Singer, A Friedmann, *Cybersecurity and cyber war – What everyone needs to know* (OUP 2014) 13; K Kittichaisaree, *Public international law of cyberspace* (Law, Governance and Technology Series vol 32, Springer 2017) 2.

191 An inclusive definition is provided by von Heinegg who describes cyberspace as 'the globally-interconnected digital information and communications infrastructure' in W H von Heinegg, 'The Tallinn Manual and international cyber security law' (2012), 15 Yearbook of International Humanitarian Law 3, 5.

192 K Kittichaisaree (n 190) 2. Hobe understands the nexus between cyber and space mainly as the capacity of satellites to connect to the internet. S Hobe, 'The International Institute of Space Law assumes responsibility for questions of cyber law' (2017) 66.4 ZLW 647, 654–55.

193 Convention on Cybercrime of the Council of Europe (opened for signature 23 November 2001, entered into force 1 July 2004) ETS 185 (hereinafter Budapest Convention). The Budapest Convention is the first multilateral agreement relevant to cyber law. In Art. 1a and 1b it only refers to computer systems and computer data as constituents of cyber infrastructure. *See* more on the Budapest Convention in A M Weber, 'The Council of Europe's Convention on Cybercrime' (2003) 18 Berkeley Technology Law Journal 425.

194 EU NIS 1 Directive (n 153) art 1.1 describes its subject as 'achieving a high common level of security of network and information systems'.

195 D Livingstone, P Lewis, 'Space: The final frontier for cybersecurity?' (*Chatham House*, 22 September 2016) <https://reader.chathamhouse.org/space-final-frontier-cybersecurity> 2-3; Potter refers to the transmission, reception and storage of information through telecommunications in M Potter, 'Outer space cyberspace nexus: Satellite crimes' in *Proceedings of the thirty-seventh Colloquium on the Law of Outer Space* (AIAA 1995) 55.

196 P J Blount, 'Satellites are just things on the Internet of Things' (2017) 42.3 ASL 273, 278.

the term 'cyber' will be used to describe any activity that takes place within a NIS involving a space-related component, be it on the Earth or in outer space.

Considering this definition of the term 'cyber', the cyber element of space activities is not only present in outer space or connected only to space objects. A great part of space cyber infrastructure encompasses ground objects, which become a *de facto* part of space activities, as far as cyber issues are concerned. This is particularly the case with space big data, where ground infrastructure is an indispensable part of the space big data cycle.[197]

– *The cyber element of space big data*

The cyber element is involved in various stages of space big data and their applications. Given that space big data are often generated for specific applications or to be made available further to other users, they undergo a cycle of movement among devices and users. This chain of data transfer relies on several stages of cyber infrastructure.[198] First, in the data collection and generation process the communication between the collecting or generating device and the receiving system is conducted via cyber means. This can involve the connection between satellites and ground stations or a satellite with another satellite, as well as the direct access of an external user to the said device. Second, the storage of data at the receiving device on board a space object or at a ground station is also realised by cyber means. This storage includes the safeguarding of digital information within the device, as well as the connection of this device to other storage devices and its users. Third, the data process involves cyber operations in the connection between the processing system and the system from which the data is derived and to which the data are further transmitted, as well as the processing software deployed for that cause. Finally, data distribution and redistribution are often conducted via cyber systems through the connection of remote devices, mainly via internet networks. The reliance on cyber infrastructure comes in the form of the transfer of space data through connected devices, the internet, and other information networks.

The stages described above roughly represent the cycle that space big data concludes. Except for involving themselves cyber technology, these stages are also cyber-connected to the respective preceding and succeeding stages. For instance, the collection of space big data is connected to the storage of space

197 Similar is the opinion expressed in the Tallinn Manual supporting that activities on the Earth may qualify as space activities when they encompass activities or effects that take place in outer space. M N Schmitt, *Tallinn Manual 2.0 on the international law applicable to cyber operations* (CUP 2017) 272.

198 More on the transfer of data within satellite systems, J Fritz, 'Satellite hacking: A guide for the perplexed' (2013) 10.1 Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies 21, 21–22.

big data through the use of cyber infrastructure. Consequently, the cyber element of space big data is present in all stages of their lifecycle and varies according to the type of applications and uses for which space big data are employed. The application of relevant cybersecurity regulations depends on the part of the data cycle that falls under the protective scope of the given law. Given the above, cybersecurity is relevant for EO data, GNSS data, satellite-based internet data, as well as astronomy and other space-related data.

– *Cyber threats against space big data*

Cyber infrastructure enables a significant part of the space big data lifecycle, but at the same time can expose data to threats of unauthorised use and access. The successful undertaking of space big data applications relies on two main premises, namely that data are made available as required for the purposes of a specific use and that these data can be accessed solely by authorised parties. Cybersecurity threats are linked to the vulnerability of datasets to external and unauthorised attacks, mostly carried out through access to network systems and interference with the stored data. Such threats are a considerable concern for satellites and other connected systems, given their growing integration with internet technology and the transmission of various sorts of data.[199] To mention but a few, risks to space big data security could disrupt services, such as navigation and banking transactions, affect transportation, and reveal confidential information.[200] The threats examined below refer to the security of data with regard to their confidentiality, integrity, and availability.[201] Any action aiming at undermining these qualities constitutes a cyber threat.

There are various motives behind threats to the security of space data. Considering the abundance of uses and applications of satellite technology involving space data, the consequences of security threats and breaches can vary accordingly. The analysis at hand is based on motives that are not related

199 M Bartels, 'Why satellites need cybersecurity just like you' (*Space.com,* 10 December 2018) < https://www.space.com/42658-cybersecurity-for-satellites.html>; D P Fidler, 'Cybersecurity and the new era of space activities' (*Council on Foreign Relations,* 3 April 2018) <https://www.cfr.org/report/cybersecurity-and-new-era-space-activities>.

200 T Roadnight, 'Space: The final frontier for cybersecurity?' (*Nexor*) <https://www.nexor.com/blog/space-final-frontier-cybersecurity>.

201 J Kosseff, 'Defining cybersecurity law' (2018), 103 Iowa Law Review 985, 995. These characteristics are also mentioned in several legal documents including EU NIS 2 Directive (n 153) art 6.2 and IoT Act (n 173) sec 2.9. They are also referred to in the UNODC Comprehensive Study on Cybercrime of 2013 <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> 11.

to aggression, use of force, attack, or warfare.[202] Without disregarding the malicious character of cyber operations carried out for purposes amounting to force or attack, as defined in international humanitarian law, the growing commercialisation in the field of space big data creates fertile ground for cyber risks of mainly financial and similar non-aggressive motives.[203] A distinction is made between cyber threats against stored data and cyber threats against transmitted data. Even though interference with data transmission can have equally disruptive results, data storage is the most vulnerable part, since it has more severe consequences for data than the disruption in transit,[204] both in terms of potential damage or loss, as well as in terms of duration of occurrence.

The main difference between the storage in databases located on the ground and those located in outer space is the ease of access to the contained data. Whereas Earth-based storage is open to physical as well as electronic cyber threats, the same is not valid for space-stored data, which due to remoteness, technology, and costs involved, are not as vulnerable. Since the success of space data applications is strongly connected to the security of these data, it is worth observing whether relevant regulations provide sufficient safeguards depending on the location of the data storage or other factors.

3.4.3 Preliminary conclusions on the cybersecurity implications of space big data

The cyber domain incorporates the immaterial dimension of information technology networks, which enable and connect all stages of the space big data lifecycle. Cybersecurity safeguards the availability, authenticity, integrity, and confidentiality of these networks and the information contained therein. Given the importance of maintaining a consistent flow of reliable data for the use of space big data, all types of space data are affected by cybersecurity laws.

This high-level analysis of the EU cybersecurity framework, in conjunction with the national framework of the US, indicates that the cybersecurity protection of space big data depends on whether they fall under the definition of a NIS and whether the prescribed cybersecurity measures are relevant to

202 Kittichaisaree (n 190) 153. Furthermore, cyber threats might not associate to the principle of exclusively peaceful uses of outer space, whether the term is interpreted as non-military or non- aggressive. K U Schrogl, J Neumann, 'Article IV' in S Hobe, B Schmidt-Tedd, K U Schrogl (eds), *Cologne Commentary on Space Law – Volume 1: Outer Space Treaty* (Berliner Wissenschafts-Verlag 2009) 82.

203 On regulating cyber space as field of economic activity, *see* M E O'Connell, 'Cyber security without cyber war' (2012) 17.2 Journal of Conflict and Security Law 187, 203.

204 M Mejia-Kaiser, 'Space law and unauthorised cyber activities' in K Ziolkowski (ed), *Peacetime regime for state activities in cyberspace – International law, international relations and diplomacy* (NATO CCDCOE Publication 2013) 350-351.

the space big data lifecycle. When cybersecurity regulations apply to space big data, they affect all the identified types of space data, namely EO data, satellite-based location data, satellite-enabled connectivity data, and astronomy and other space-related data.

3.5 Export control

Space data represent the most prominent example of growth in commercial space activities and are expected to grow in terms of their volume and uses.[205] Their abundant potential combined with the ease of access to open and commercial data sources have created a fertile environment for further development. The latter also depends on the continuation of access to and dissemination of space data, which are in turn reliant on the broad exchange of space data and the involvement of private actors. However, export regulations limit the cross-country transfer of space technology on the grounds of its dual-use. Export control is based on the premise that space technology can be used simultaneously for both civil and military purposes. It is relevant to space big data since they rely heavily on data access and distribution. Among the items that may be covered by export limitations are satellites and satellite systems that generate data, data, and datasets, as well as technologies used in space big data analysis.

This section examines the applicability of export control regulations to space big data, with a particular focus on the storage and transfer of EO data. Section 3.5.1 focuses chiefly on the EU regime, but also analyses the US regime, given its far-reaching scope and extra-territorial application. Section 3.5.2 studies the connection between space big data and export control.

3.5.1 Export control in the space sector

Export control refers to the instruments and processes that limit the distribution of items and technology that are sensitive, in terms of national and international security.[206] In particular, it covers tangible and intangible assets that can be considered of dual use or as weapons. Export control also involves the

205 'Towards a $7.5b Earth observation data & service market by 2030' (*Euroconsult*, 6 October 2021)<https://www.euroconsult-ec.com/press-release/towards-a-7-5b-earth-observation-data-service-market-by-2030/>. Export control was the topic of a thesis conducted in the framework of the Advanced Master in Air and Space Law at Leiden University and was considered for the analysis in this section. D Stefoudi, *Export control and dual-use of space technology: legal and policy considerations: a comparative analysis of the current international export control regimes with emphasis on E.U. and U.S. legislation* (Leiden University 2016).

206 Y Aubin, A Idiart, *Export Control Law and Regulation Handbook* (1st edn, Kluwer Law International 2007) 4.

obligations stemming from international agreements to limit the dissemination of dangerous items. Space technology is of dual-use character, meaning that the same instruments can be used both for civil and military purposes, whereas part of the space sector is dedicated to military and defence uses. It is this dual-use character and military extensions of space technology that form the subject of export control.[207]

Space big data rely on the exchange of technology, products, and know-how, which may occasionally fall under export limitations. The most common example is the need to access dual-use satellites that generate, store, and distribute data. States may impose limitations to such technology on the grounds of security, as well as in order to protect their economic and foreign policy interests. Export rules are enforced by national authorities, apply to national and legal persons within a certain jurisdiction, and concern destinations and users outside them.

'Export' refers to the transfer, shipment, or transmission of regulated goods.[208] It entails the shipment, the electronic or digital transmission, the release or disclosure verbally or by means of inspection, as well as the use or application on behalf or for the benefit of others. Each export regulation specifies the exact meaning of export under its scope. In US laws, export is defined as a shipment or transmission,[209] or is also extended to transfer, change of registrations, control or ownership, oral and visual disclosure, as well as performance on behalf of another person.[210] Under EU law, the territorial application of export rules extends to the borders of all Member States, hence export mainly refers to transfers outside the EU.[211] It also refers to transmission by electronic means of any sort, as well as verbal disclosure, when carried out via telephone.[212]

Due to the broad impact of export control, covering several technologies used in the space sector, it can have significant effect on the exchange among countries. Export rules govern two categories of space technology, dual-use technology and munitions.

207 R Gonzalez Aninat, 'UNISPACE III: An expression of diplomacy for development' in P Gasparini Alvares (ed), *Evolving trends in the dual use of satellites* (UNIDIR 1996) 166.

208 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) [2021] OJ L206/1 art 2.2 (hereinafter EU Regulation on Export Control). 15 CFR § 772.

209 15 CFR §772.

210 22 CFR §120.17.

211 Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code [1992] OJ L 302/1 art 161.

212 EU Regulation on Export Control (n 208) art 2.2.

– *The EU export control regime*

The European framework on export control is primarily focused on dual-use items and technologies. Munitions are regulated on the level of Member States, since the mandate of the European Union in this regard is limited. On the European level, export controls are governed by Regulation 2021/821 on setting up a Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items, which constitutes an amendment of previous similar Regulations.[213] The main purpose of this Regulation is to establish an EU-wide regime for the export of dual-use items. Among those that concern space technology are the export rules covering the aerospace sector, defence, navigation, and telecommunications technologies.[214]

The Regulation calls for an effective control mechanism, while maintaining a level-playing field for the European industry. Whereas the basis of the EU Export Control Regulation is national sovereignty, it also aims to ensure a level of free movement of dual-use items across the EU. Member States can introduce stricter measures compared to the EU Regulation.[215]

The Regulation provides for the export licensing procedure, which is managed either by the EU or the Member States, customs requirements, as well as cooperation among the competent EU and national authorities.

Its Annexes include various lists of the dual-use items covered by the Regulation, samples of authorisation forms, and amendments.[216]

(a) Controlled dual-use items

Article 2.1 of the Regulation defines dual-use items as items, including software and technology, which can be used for both civil and military purposes. These items are listed in Annex I of the Regulation and require an export authorisation, according to Article 3. The list of controlled items is divided into ten categories and items related to space technology are mainly included in Category 9 'aerospace and propulsion'. Additionally, items related to space technology and space big data can be found in other categories, especially in Category 3 'electronics', Category 4 'computers', Category 5 'telecommunications and information security', Category 6 'sensors and lasers', Category 7 'navigation and avionics', and Category 0 'nuclear material'. The items included in the dual-use list are controlled when they are to be transferred individually or as part of another object. Whether a controlled item is a signi-

213 EU Regulation on Export Control (n 208).

214 Green Paper – The dual-use export control system of the European Union: Ensuring security and competitiveness in a changing world COM(2011) 393 final.

215 R Rosanelli, 'Seeking harmonisation: European space export control at the crossroads – ESPI Perspective 54' (*ESPI,* November 2011) <https://www.files.ethz.ch/isn/136417/ESPI_Perspectives_54.pdf> 4.

216 The Annexes include various lists of the dual-use items covered by the Regulation, samples of authorisation forms and amendments

ficant part of another object depends on several factors, among which are its quantity and the technological knowledge it required. As an indication, publicly available software or controlled objects that require minimal integration effort do not fall under the scope of the Annex.[217]

Compliance with the EU export control framework requires technical knowledge, to identify whether and in which category of controlled items a given item may belong. Some of the instances where space big data may be affected by export control include: data-based referenced navigation (Category 7), satellite navigation systems (Category 5 and 7), electronic items designed for signal processing (Category 3), computers and assemblies for signal processing and image enhancement (Category 4), communication equipment on board satellites (Category 5), information security systems designed for cryptography (Category 5 and 7), space-grade optical sensors and detectors (Category 6), radar systems (Category 6), navigation equipment (Category 7). In addition, several elements described in Category 9 are of relevance to space big data, such as spacecraft and equipment related to payload data handling, as well as control systems and equipment for acquiring and processing data in real-time. Furthermore, Category 9 items related to the testing, construction, and operation of spacecraft can be of relevance, since they affect the development of satellite systems involved in space big data.

The EU has also issued a Regulation concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine that limit virtually any export of space-related technology, including the supply of products and assistance, but maintaining intergovernmental cooperation in space programmes.[218]

(b) Exporting dual-use items

The EU export control Regulation applies to the export of dual-use items. Article 2.2 of the Regulation defines export as an export procedure,[219] a re-export,[220] and an outward processing procedure,[221] all of which imply the transfer of European Union goods outside the EU customs territory. The definition also includes the transmission of software or technology by electronic media, making them available in an electronic form or transmitting them orally

217 EU Regulation on Export Control (n 208) annex I.

218 Council Regulation (EU) 2022/879 of 3 June 2022 amending Regulation (EU) No 833/2014 concerning measures in view of Russia's actions destabilising the situation in Ukraine [2022] OJ L 153/53.

219 By reference to Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (recast) [2013] OJ L 269/1. Export is described as Union goods taken out of the customs territory of the Union.

220 Re-export is the procedure of non-union goods being taken out of the customs territory of the Union.

221 Under the outward processing procedure, Union goods may be temporarily exported from the customs territory of the union, in order to undergo processing.

when described over a voice transmission medium. The Regulation addresses mainly exporters, but can also apply to providers of brokering services and providers of technical assistance. An exporter, according to Article 2.3 holds the contract and has the power to determine the sensing of the items, decides or makes available the transmission of software and technology by electronic means, or carries the dual-use item. A brokering service, per Article 2.7, is the negotiation or arrangement of transactions, or the sale or purchase for transfer, while technical assistance, per Article 2.9, covers any technical support and technical service. Exporters, providers of brokering services, and providers of technical assistance can be natural persons, legal persons, or partnerships.[222]

According to Article 3 of the Regulation, in order to export a dual-use item listed in the Regulation, authorisation is required from the exporter, and occasionally the provider of brokering services or technical assistance. The types of authorisations that are required vary according to the type of item and the country of destination and are described in Article 12. An individual export authorisation is granted to a specific exporter for a specific end-user and covers one or more items that are destined for a specific country.[223] A global export authorisation is granted to a specific exporter for one or more users and covers a type or category of items that are destined for one or more countries.[224] The individual export authorisation and the global export authorisation are issued by the country where the exporter is resident or established.[225] If the exporter is not established in the European Union, the authorisation is issued by the country where the dual-use item is located.[226] The competent authority may decide on additional requirements for these authorisations, such as an end-use statement or an internal compliance programme.[227]

Except for the general types of authorisations, the Regulation provides for two additional types with a broader scope. A national general export authorisation is issued by national authorities of EU Member States, under conditions included in the national laws of the EU Member State where the competent authority is located,[228] and covers dual-use items in Annex I. A Union general export authorisation allows the exporter to export dual-use items to certain

222 EU Export Control Regulation (n 208) art 2.3(a), 2.3(b), 2.8, and 2.10.
223 EU Export Control Regulation (n 208) art 2.12.
224 EU Export Control Regulation (n 208) art 2.13.
225 EU Export Control Regulation (n 208) art 12.2.
226 EU Export Control Regulation (n 208) art 12.2
227 EU Export Control Regulation (n 208) art 12.4. An internal compliance programme (ICP) is defined in Article 2.21 as the policies and procedures that are adopted by the exporters to ensure compliance with the Regulation.
228 EU Export Control Regulation (n 208) art 2.16. A national general export authorisation should include the elements listed in Section C of Annex III.

destinations.[229] Both types of authorisations should meet the requirements listed in Sections A to H of Annex II. These requirements concern exports of certain categories of items to certain destinations. Exports to, among others, the US, the UK, Switzerland, Australia, and Canada can be conducted under a Union general export authorisation, which facilitates exports of one or more categories under a single authorisation process.[230] Both types of authorisation cover the dual-use items listed in Annex I of the Regulation but exclude the items listed in Section I of Annex II, which are some of the more sensitive dual-use items.

Furthermore, the Regulation requires authorisation for items that are not listed in Annex I that are used for cyber-surveillance, if they are deployed in connection with violations of human rights and humanitarian laws.[231] It also entrusts competent national authorities in EU Member States to restrict the export of items that may be used as weapons or for military purposes[232] and Member States to adopt additional measures for similar occasions.[233]

Once the appropriate authorisation has been obtained, the exporter should present such proof when completing the formalities at the responsible customs office.[234]

– *The US export control regime*

The US export control framework is similar to the EU framework, in that it also relies on a list of controlled dual-use items. However, it differs as it involves a list of munitions as well. It primarily relies on two pieces of regulation, namely the Export Authorisation Regulations (EAR)[235] and the International Traffic in Arms Regulations (ITAR).[236] EAR focuses on the transfer of dual-use items and technologies and is monitored by the Department of Commerce Bureau of Industry (BIS). ITAR focuses on defence articles and services and falls under the Directorate of Defence Trade Controls (DDTC) of the Department of State. Despite their differences, both EAR and ITAR rely

229 EU Export Control Regulation (n 208) art 2.15.
230 EU Export Control Regulation (n 208) annex II sec A.
231 EU Export Control Regulation (n 208) art 5.
232EU Export Control Regulation (n 208) art 4.
233 EU Export Control Regulation (n 208) art 9 and 10. More information about the national measures and procedures adopted by EU Member States, according to the regulation can be found in Information Note Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (OJ L 206, 11.6.2021, p. 1.): Information on measures adopted by Member States in conformity with Articles 4, 6, 7, 9, 11, 12, 22 and 23 2023/C 208/06 [2023] OJ C 208/1.
234 EU Export Control Regulation (n 208) art 21.
235 Export Administration Regulations 15 CFR §730-774 (hereinafter EAR).
236 International Traffic in Arms Regulations, 22 CFR §120-130 (hereinafter ITAR).

on the same basis, namely the U.S. President's discretion to decide on matters of dual-use and munitions export.[237]

ITAR is laid down in paragraphs 120-130 of Title 22 'Foreign Relations' of the Code of Federal Regulations. Under ITAR licenses are only provided to U.S. natural or legal persons. Only as an exception, authorisation can be granted to a non-U.S. government entity with an establishment in the country, and a foreigner for the purpose of either re-export or re-transfer of controlled items or brokering services. ITAR applies to the items included in the Munitions List of twenty-one categories. Its provisions apply to US citizens, as well as to foreign nationals when they use U.S. technology, which is referred to as extraterritoriality element.[238] In 2014 the U.S. Government relaxed some ITAR regulations by removing commercial satellites from the Munitions List and placing them under the scope of EAR.[239]

EAR is described in Articles 730-774 of Title 15 of the U.S. Code of Federal Regulations and governs the export of dual-use items. They apply to the export and re-export of the items included in the Commerce Control List. To determine whether an export is permitted, the controlled item and the destination country are taken into account. Following the said 2014 reform, most commercial satellites fall under the provisions of EAR. In order to identify whether a controlled object is of US origin and the provisions of EAR apply, the *de minimis* requirement is factored in. The requirement refers to the percentage of US technology incorporated in a controlled item.[240]

Similar to the EU export control regulation, the controlled items that are relevant to space big data can be found in ITAR Categories IV and XV which include launch vehicles, spacecraft, sensors, and radars that are used in systems collecting and transmitting space big data. Category IX includes military electronics and makes specific reference to synthetic aperture radar and images with resolution better than 30cm, while Category XII encompasses most parts of GNSS systems and receiving equipment.[241] EAR includes items related to space big data in Category 3 on electronics, Category 4 on computers, Category 5 on telecommunications and information security, Category 7 on navigation, as well as Category 9 on aerospace and propulsion.

---

237 J Crook, 'National insecurity: ITAR and the technological impairment of U.S. national policy' (2009) 74 Journal of Air Law and Commerce 505, 516.

238 R Rosanelli, *US export control regulations explained to the European exporter: A handbook* (University of Liege European Studies Unit 2014) 4-5.

239 US Department of Commerce, Space Export Control Updates <https://www.bis.doc.gov/index.php/forms-documents/doc_view/724-space-export-controls-update>.

240 De Minimis Rules and Guidelines (as modified on 5 November 2019) <https://www.bis.doc.gov/index.php/documents/pdfs/1382-de-minimis-guidance/file>.

241 Guidance related to 'foreign access to United States space-based PNT capabilities' can be found in section 6 of the Memorandum on Space Policy Directive-7 – The United States Space-Based Positioning, Navigation and Timing Policy (2021).

The US Office of Foreign Assets Control (OFAC)[242] may also impose limitations based on sanctions on designated countries. Under that, US companies and individuals cannot perform transactions with counterparts from the sanctioned countries in specific fields of activity.[243]

Except for the EU and the US regimes, export control is also driven by international agreements, such as the Wassenaar Arrangement that limits the export of military and dual-use items.[244] The provisions of the Wassenaar Arrangement are included in the EU and the US regime and are also applicable to other State parties.[245]

3.5.2 Export limitations for space big data

Space activities, including space big data, are collaborative by nature and rely on States being able to exchange items and expertise. Export control offsets some of the cooperation and freedom provisions laid down in international space law, but the numerous military extensions of space technology justify some of these limitations.[246] Military uses of space technology include military communication through satellites, early warning services via ballistic missile defence surveillance systems, reconnaissance satellites monitoring arms traffic and other crises, military uses of weather satellites, navigation, and positioning, as well as the deployment of remote sensing satellites for military objectives.[247] Several of these capabilities are supported by space data and reveal the distinguishing features of space technology that is able to simultaneously

242 Office of Foreign Assets Control <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>.

243 Sanction Programs and Country Information <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information>.

244 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1996). Other international agreements that affect exports are the Missile Technology Control Regime that limits exports of components used in missiles and unmanned aerial vehicles <https://mtcr.info/>, the Nuclear Suppliers Group regarding the proliferation of nuclear technology <https://www.nuclearsuppliersgroup.org/en/>, and the Australia Group on control of chemical and biological weapons <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html>. Even though they are relevant to space technology, in terms of items and materials used in the manufacturing of satellites, they are not directly relevant to space data.

245 The Wassenaar Arrangement has 42 State parties <https://www.wassenaar.org/participating-states/>.

246 M Mowthorpe, *The militarization and weaponization of space* (Lexington Books 2004) 3 ; J Kingwell, 'The militarization of space - A policy out of step with world events' (1990) 6.2 Space Policy 107, 107-108.

247 S Pace, 'Economic interests and military space systems: An American perspective' in P Gasparini Alvares (ed), *Evolving trends in the dual use of satellites* (UNIDIR 1996),139.

combine civil, commercial, and military aspects.[248] The growing commercialisation of the space sector, including in the field of space data, may decrease the tendency to use space technology for military purposes.

The intended use of space big data can be difficult to distinguish, given the variety of applications they may find. Therefore, it is difficult to determine in advance, whether space big data as such are of dual-use and control their export. An example of the potential dual-use of space data can be found in the EU flagship programs, Galileo and Copernicus, based respectively on geopositioning and EO data, which were established to provide Europe's independence in navigation services and Earth monitoring.[249] Galileo aims to offer improved tracking services for a variety of uses and emergency response but includes conditions in the provision of high-accuracy services. Copernicus offers satellite data to be used in several applications based on full, free, and open access, but its data policy foresees limitations based on, among others, security.[250] While the purpose of both missions is primarily civilian, their data policy acknowledges the potential security implications of the positioning and remote sensing data they offer.[251] Likewise, SSA data can have dual-use extensions, both in terms of the satellites that are used to collect and transmit data and the objects that the data track.[252] At the moment, space big data applications are based on less sensitive data, such as low and medium-resolution data or open-access data, which are not impacted by export control. However, the increasing offer of high-resolution EO data and sophisticated data analytics may revive dual-use considerations about space big data. For similar reasons, sophisticated technology that may be controlled or be used for dual-purposes, and export control may also affect satellite-based internet data.

248 M Mineiro, *Space technology export controls and international cooperation in outer space* (Springer 2012) 4.

249 M Aliberti, A Lachen, 'The future of European flagship programmes in space – ESPI Report 53' (*ESPI*, November 2015) <https://www.espi.or.at/wp-content/uploads/espidocs/Public%20ESPI%20Reports/ESPI_Report_53.pdf> 4.

250 EUSPA Regulation (n 29) art 53.1(b).

251 The Copernicus program was previously named Global Monitoring for Environment and Security.

252 Y Otani, N Kohtake, 'Applicability of civil and defense dual use to space situational awareness systems in Japan' (2019) 47 Space Policy 140, 142 and 144-146; A Azcárate Ortega, 'Not a rose by any other name: Dual-use and dual-purpose space systems' (*Lawfare*, 5 June 2023) <https://www.lawfaremedia.org/article/not-a-rose-by-any-other-name-dual-use-and-dual-purpose-space-systems>.

3.5.3 Preliminary conclusions on the implications of export control on space big data

Export control aims to balance concerns over national security with facilitating commercial growth in the space sector. States may be reluctant to share technology that is sophisticated and possibly harmful to their security and financial interests, but further advancements in the space sector call for their wider distribution.[253]

The main connection between export regulations and space big data stems from technology that is required to collect and analyse space big data, such as computer software and sensors that fall under lists of controlled dual-use items. In turn, this can affect cooperation among public and private entities that are found in different countries, as well as access to foreign technology. Export limitations become relevant when considering the public and private entities that maintain infrastructure or offer services in more than one country. At the same time, companies located in different countries that cooperate in providing business solutions, as well as their users that may be nationals of different States can be impacted.

Space big data rely on the interoperability and exchange of data, which often take place cross-border. Any limitation to the dissemination of information, especially given the speed and volume in which data are generated, moved, and distributed, will affect the space big data lifecycle. Against this backdrop, export regulations can affect all types of space big data. However, due to their nature, some types of space data raise less concerns in terms of their dual-use applications. In particular, GNSS data for civil uses and astronomy data are less likely to present export control implications. In any event, export controls affect the technology that is used to collect, process, and store space data, rather than space data themselves.

3.6 Data policies relevant to space big data

Alongside the UN Space Treaties and information-related laws that are relevant to space activities, documents governing the collection, access, use, and dissemination of space data in various contexts can find applications to space big data. Data policies are documents of regulatory character, binding and non-binding, which establish the conditions under which space data can be

253 Along these lines, the Satellite Industry Association provided recommendations for remote sensing policies that promote competitiveness and take into account the commercialisation of the space sector. Satellite Industry Association Earth Observation Forum Working Group, 'White Paper – National Security Policy Directive 27 and U.S. Commercial Remote Sensing Policy' (*Satellite Industry Association*) <https://sia.org/wp-content/uploads/2022/10/White-Paper22-National-Sec-Policy-Dir-27-and-US-Commercial-Remote-Sensing-Policy.pdf>.

collected, used, and disseminated. They are adopted on international, regional, and national levels and provide different requirements for the collection, access, use, and dissemination of the space data under their scope. Section 3.6.1 analyses the data policy of the EU Space Programme and particularly of Copernicus, one of the first missions dedicated to EO big data. Section 3.6.2 includes the data policies of ESA and NASA for space data from their missions. Section 3.6.3 studies national data policies from EU and non-EU countries, with emphasis on The Netherlands and the Dutch Satellite Data Portal. Section 3.6.4 addresses the UN Remote Sensing Principles that are dedicated to EO data, primarily for environmental monitoring and natural disasters.

Except for these policies that stem from States, space agencies, or international organisations, there are a number of data policies imposed by the suppliers of space data on a commercial level, commonly in the form of user license agreements. These policies vary, according to commercial interests and data availability, and are determined by the supplier, following potential national or other data policies that may be in place.[254] Since they are not uniform, they are often not publicly available and are determined on a case-by-case basis, they are not part of the present analysis. They are addressed briefly in section 4.7, in the scope of the data that are supplied to users through the Satellite Data Portal of the Netherlands Space Office.

3.6.1 Data policy of the EU Space Programme: The EU Copernicus flagship programme as an example of space big data supply

The EU Space Programme is governed by Regulation 2021/696 of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme.[255] The EU Space Programme generates all major categories of space data, namely Earth observation data, satellite-based location data, and satellite-enabled connectivity data, as well as space situational awareness data. It comprises several components,[256] namely the Galileo global

254 Several user license agreements can be found online. For reference, some issues that are addressed in these policies and agreements are mentioned in the US Group on Earth Observations, 'Best Practices Background Document' (3 May 2021) <https://usgeo.gov/uploads/Best%20Practices%20Background%20Document_10%20May.pdf>. An overview of pricing and access policies for EO data can be found in S S Elbakry, 'Pros and cons of data pricing policies' (2023) 48.6 ASL 527, 537-541 and R Harris, R Krawec, Earth observation data pricing policy (1993) 9.4 Space Policy 299.

255 EUSPA Regulation (n 29).

256 EUSPA Regulation (n 29) art 3.1, EU Regulation. The IRIS^2 constellation will be part of the EU Space Programme, as agreed by the European Parliament and the European Council. 'Welcome IRIS$^{2.}$ Infrastructure for resilience, interconnectivity and security by satellite' (*European Commission*, 17 November 2022) <https://defence-industry-space.ec.europa.eu/welcome-iris2-infrastructure-resilience-interconnectivity-and-security-satellite-2022-11-17_en>.

GNSS constellation,[257] the EGNOS regional GNSS system,[258] the Copernicus EO system,[259] the EU Space Situational Awareness (SSA) System,[260] the GOVSATCOM satellite communication service,[261] and the IRIS^2 satellite connectivity system.[262] Galileo and EGNOS are designed to provide state-of-the-art and secure positioning, navigation, and timing services. Copernicus delivers accurate and reliable EO data and data services. The SSA system aims to enhance the capabilities of the EU in this domain, whereas GOVSATCOM makes available reliable, secure, and cost-effective communication services. The IRIS^2 constellation for secure connectivity is the latest addition to the EU Space Programme and is being under development at the time of the writing of this thesis.[263] Each of the components of the EU Space Programme involves the generation and dissemination of space data, according to their respective objectives,[264] and provides access to its data and services on varying terms.

– *Galileo, EGNOS, SSA*

The *Galileo* system entails several services, as described in Article 45.1 of the EUSPA Regulation. The Galileo *Open Service* (OS) system is free of charge and provides satellite-based location data for navigation. The Galileo *High Accuracy Service* (HAS) is free of charge and targets professional and commercial users of satellite-based navigation. The Galileo *Public Regulated Service* (PRS) is free for the EU Member States, the European Commission, the EU Council, the External Action Service, and EU agencies. The public services may be charged for other users, and they target governments and authorised users of sensitive applications. Finally, the Galileo Search and Rescue Service (SAR) is free and provides satellite-based location signals and warnings for natural disasters and other emergencies.

The conditions under which the *Open Service* of Galileo is operated and offered to its users are laid down in the dedicated Service Definition Document (Galileo OS SDD).[265] The Galileo OS SDD provides an overview of the Galileo Open Service System and its parameters, which are described on the level of their minimum performance, based on informed usage assumptions. Among

257 EUSPA Regulation (n 29) art 1a.
258 EUSPA Regulation (n 29) art 1b.
259 EUSPA Regulation (n 29) art 1c.
260 EUSPA Regulation (n 29) art 1d.
261 EUSPA Regulation (n 29) art 1e.
262 The IRIS^2 constellation is not part of the EUSPA Regulation, as it was introduced after this Regulation was adopted. It is governed by Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027 [2023] OJ L79/1 (hereinafter IRIS^2 Regulation).
263 IRIS^2 Factsheet (*European Commission*) <https://defence-industry-space.ec.europa.eu/system/files/2023-03/IRIS%C2%B2_Factsheet%20%28EN%29.pdf>.
264 EUSPA Regulation (n 29) art 4.2.
265 European GNSS (Galileo) Open Service Definition Document (Issue 1.3, November 2023).

the parameters worth noting are the purpose of the Galileo Open Services, namely their use for non-safety critical purposes, and the liability disclaimer. According to the latter, the EU and the entities that cooperate in the framework of the Galileo Open Services do not assume liability in terms of -among others- service availability, continuity, accuracy, reliability, and fit-for-purpose performance.

Likewise, the Galileo *High Accuracy Service* operates based on an Interface Control document (Galileo HAS SIS ICD),[266] which describes the technical process through which the service is offered. It also describes the terms under which the use of the service is authorised. Authorisation only allows the use and storage of technical data, and the reproduction of the HAS SIS CID. According to the HAS SIS ICD, no liability is assumed for the accuracy, completeness, or usefulness of the information in the document, nor any damage resulting from the use of the document. Moreover, the methods described in the HAS SIS CID to decode the Galileo signal and obtain its data are subject to specific terms. As far as IP rights are concerned, all rights remain with the European Union and cannot be acquired by authorised users. The HAS SIS CID and its content are copyrighted, whereas the methods for signal retrieval are patented. Finally, authorised users are required to perform according to international law, including export controls.

The Galileo *Search and Rescue* service functions according to the SAR/Galileo Service Definition Document (SAR SDD).[267] The purpose of the document is to describe the contribution of Galileo to Cospas-Sarsat, which is the process of upgrading GNSS satellites with search and rescue systems, and to present the Galileo SAR characteristics. The document is mainly technical, and the only relevant user provision is the no warranty clause regarding the availability, continuity, accuracy, integrity, reliability, and fitness of the signal and service.

EGNOS is the European Geostationary Navigation Overlay Service. Its operation of EGNOS is described in Article 46 of the EUSPA Regulation. EGNOS provides services for improved GNSS performance and is free of charge. The EGNOS Open Service Service Definition Document (OS SID)[268] describes the operation of the system and terms of use. Similarly to the other components of the EU Space Programme, there is no guarantee of availability, integrity, continuity, accuracy, reliability, or fitness for the purpose of EGNOS.

The operation of *GOVSATCOM*, which stands for Governmental Satellite Communications, is described in Article 63 of the EUSPA Regulation. GOVSATCOM is free for institutional and governmental entities unless otherwise provided.

266 Galileo High Accuracy Service Signal-In-Space Interface Control Document (Issue 1.0, May 2022).

267 SAR/Galileo Service Definition Document (Issue 2.0, January 2020).

268 EGNOS Open Service Service Definition Document (version 2.3, 2017).

The *SSA* services are described in chapter I of Title VIII of the EUSPA Regulations. The Space Surveillance and Tracking (SST) sub-component of the SSA services entails collision risk assessment between spacecraft and debris, detection and characterisation of fragmentations, breakups and collisions, risk assessment of uncontrolled re-entry, as well as preparation for debris remediation and mitigation methods.[269] The SST sub-component relies partially on space data from SST sensors.[270] SST services are free of charge and available at any time without interruption.[271] Access to SST services depends on the categories of SST users.[272] Access to all services is provided to core users, namely the EU Member States, the EU External Action Service, the EU Commission, the EU Council, EUSPA, and EU spacecraft owners. Access to all services, except collision assessment, risk assessment, and avoidance alert, is provided to non-core users, namely EU public and private entities. Access to all services upon agreement between the EU and the respective States can be provided to third parties.

– *Copernicus EO data*

Copernicus is the EO component of the EU Space Programme. It relies on EO data from the Copernicus constellation of Sentinel satellites, EO data from third parties, and in-situ airborne, ground-based, and seaborne data.[273] It generates daily 20 terabyte of data[274] and can serve as an example of space big data, especially given the volume and variety of data it offers.

Copernicus is primarily based on a full, open, and free data policy that allows all users, without distinction between EU and non-EU citizens, public or private entities, legal or natural persons, to access and obtain the available data. Full access refers to the content of the data, which is offered in a manner that enables end-users to process them into value-added products. Open access describes data that is available and accessible to download, use, and redistribute by everyone without discrimination in terms of people or purposes. The Copernicus data are also provided on a cost-free basis. Eventual expenses might occur in case of exclusive data access or large datasets. The Copernicus data and information policy is described in Article 53 of the EUSPA Regulation. Access to Copernicus data is based on a free, full, and open data policy, as established in Article 53.1. Accordingly, the data can be used, reproduced, distributed, adapted, and modified according to the needs of their users.

269 EUSPA Regulation (n 29) art 55.1.
270 EUSPA Regulation (n 29) art 54.1(a).
271 EUSPA Regulation (n 29) art 55.2.
272 EUSPA Regulation (n 29) art 56.1.
273 EUSPA Regulation (n 29) art 49.4(a).
274 'Cool facts for your next Copernicus small talk' (*Copernicus*, 20 December 2018) <https://www.copernicus.eu/en/news/news/observer-cool-facts-your-next-copernicus-small-talk>.

Even though Copernicus data are made available through an open policy, there are reasonable concerns that justify restrictions to data access and use. The format, timeliness, and dissemination characteristics of the data are predefined, whereas licensing conditions for third-party data may be in place. Moreover, the collecting and distributing system of Copernicus data should be protected against disruptions and reliable access to Copernicus data and information should be ensured. Finally, security limitations may apply. Article 34 of the EUSPA Regulation provides for a high level of security of the ground and space infrastructure, the technology transfers, the development and preservation of Union competencies and know-how, and the sensitive classified and non-classified information. To ensure that level of security, a risk and threat analysis is performed by the EU Commission, resulting in security requirements for the components of the EU Space Programme.

The Copernicus data policy can be used as an example of conditions that relate to the collection, access, use, and dissemination of data. On the one hand, it recognises the potential of EO data generated continuously and on a large scale, hence establishing a basis for free, full, and open access. On the other hand, it takes into account limitations that may be eventually tied to the acquisition, use, and distribution of some data, and provides for a minimal level of restrictions.

– *IRIS² space-based connectivity data*

In November 2022, the European Union announced the Union Secure Connectivity Programme, IRIS², the Infrastructure for Resilience, Interconnectivity and Security by Satellite, as part of the EU Space Programme.[275] IRIS² is expected to be an operational satellite constellation by 2027 to provide secure connectivity services to governmental and non-governmental entities, across the EU and other areas around the world. It is governed by a Regulation (IRIS² Regulation) that is separate from the EUSPA Regulation that covers other components of the EU Space Programme.[276] Its objective is to offer secure services for governmental users and high-quality services for private and commercial users, reliably and cost-effectively. Although the IRIS² constellation will enter a market that is already developed by commercial actors, it aims to create autonomous capabilities for the European Union in the field of

275 G Tricco, G Zaghi, M Makurat, 'Securing communications: What to expect from the IRISS (Infrastructure for Resilience Interconnectivity Security by Satellite)' (*ITSS*, 2 January 2023) <https://www.itssverona.it/securing-communications-what-to-expect-from-iriss-infrastructure-for-resilience-interconnectivity-security-by-satellite>.

276 IRIS² Regulation (n 262).

satellite connectivity,[277] as part of the EU Space Strategy for Security and Defence.[278]

The purpose of IRIS^2 is to offer secure and autonomous space-based connectivity,[279] which makes it the only public policy so far that deals with satellite-based internet data. In particular, the IRIS^2 constellation is meant to offer less reliance on non-EU-based services through uninterrupted, secure, autonomous, reliable, and cost-effective connectivity on a governmental service basis, as well as improved connectivity on a commercial basis.

The IRIS^2 Regulation describes the portfolio of governmental services[280] that should function complementary to GOVSATCOM. The portfolio includes services based on governmental infrastructure for users that require a high level of security and quantum communication services. The portfolio also comprises services based on commercial infrastructure. The governmental services of IRIS^2 will be available to three types of users.[281] First, it will be available to EU Member States, the EU Council, the European External Action Service, and the users they authorise, namely public authorities of the EU and Member States and natural and legal persons acting on behalf of these authorities.[282] It will also be available to other EU agencies and bodies whose tasks can benefit from secure connectivity. Third countries and international organisations can also access the services, under conditions relating to international relations of the EU and based on specific agreements.[283]

3.6.2 Data policy of space agencies: The examples of ESA and NASA

The European Space Agency (ESA)[284] has several policies that relate to data collected through its missions and used within the framework of its activities. One set of policies concerns personal data that are handled in the regular operations of ESA and should comply with specific collection and processing

277 'IRIS^2: The new (material) girl on the block, ESPI Brief 61' (*ESPI*, 22 December 2022) <https://www.espi.or.at/briefs/iris2-the-new-material-girl-on-the-block/>.

278 EU Space Strategy for Security and Defence <https://defence-industry-space.ec.europa.eu/eu-space-strategy-security-and-defence_en>.

279 IRIS^2 Regulation (n 262) art 3.

280 IRIS^2 Regulation (n 262) art 10.

281 IRIS^2 Regulation (n 262) art 9.

282 IRIS^2 Regulation (n 262) art 12.

283 IRIS^2 Regulation (n 262) art 39 and 40.

284 The European Space Agency (ESA) is an intergovernmental organisation with twenty-two Member State. ESA focuses on scientific and technical research related to outer space and promotes the cooperation among its Member States and the application of space technology. More information about ESA can be found in <https://www.esa.int/>.

requirements.[285] A second set of policies concerns the scientific and technical data from ESA missions. A third set of policies relates to space data and particularly remote sensing data. A fourth set of policies concerning space data can be found in the ESA Terms and Conditions for accessing data from its EO missions. The first set of policies remains outside the scope of this thesis since it is not specific to space big data.

According to the ESA Convention and the ESA Industrial Policy,[286] ESA contracts are geographically distributed among its Member States on the basis of the States' return coefficient, as determined by the participation of States in the optional programmes of ESA.[287] This distribution affects the contracting parties that have access to data from ESA missions. The ESA Rules on Information, Data, and Intellectual Property[288] distinguish between in-house-developed and contractor-developed information, data, and intellectual property. Chapter I of the Rules concerns in-house development and allocated rights to data and information to ESA, when they are created in the scope of duties related to ESA missions, unless another specific arrangement is in place. When data and information are created outside these duties, rights over them belong to the person who created them. For in-house developed data owned by ESA, used for space research and development, its Member States have rights to access and use free of charge, on a non-exclusive basis. ESA can issue royalty-free licenses with the right for Member States to sub-license the data and information. Uses that are not related to space research and development may ensue payments of royalties to ESA or reimbursement of transfer costs, while ESA may request measures to keep these data and information confidential. Chapter II of the Rules concerns contractor development, where rights over data and information depend on whether they come from missions that are fully paid by ESA, non-fully paid by ESA, or under a partnership agreement. The ESA Rules on Information, Data, and Intellectual Property mainly refer to technical data, namely the knowledge that is not or cannot be protected

285 European Space Agency Personal Data Protection Framework <https://esamultimedia.esa.int/docs/LEX-L/ESA_Principles_of_PDP_Rules_of_Procedure_for_DPSA_and_Policy.pdf>.

286 ESA Convention and Council Rules of Procedure (8th edn, November 2019) (hereinafter ESA Convention). Article VII of the ESA Convention lays down the industrial policy of the Agency, which is further elaborated in the Industrial Policy Rules and Regulations ESA/REG/009 (1 July 2015).

287 ESA Convention (n 286) art IV. This method of geographical distribution is also referred to as fair return principle.

288 Rules on Information, Data and Intellectual Property ESA/REG/008 (23 April 2014).

by a legal title or an intellectual property right.[289] Such data do not include space data.

ESA has a specific data policy applicable to its EO missions, the ESA Data Policy for ERS, Envisat, and Earth Explorer missions.[290] The part of the policy dedicated to the legal framework dictates that ESA retains ownership, on behalf of the participating States, of all primary data, whose distribution should be consistent with the UN Remote Sensing Principles. The ESA Data Policy distinguishes between a free dataset and a restrained dataset. Under the free dataset, where the majority of data belongs, users have full and open access, free of charge, assuming that access is provided online. Access is granted upon online registration and acceptance of the ESA Terms and Conditions,[291] without requiring a specific description of the data use. Redistribution rights are granted upon request. If access is not provided online, it is subject to a project proposal regarding the use of the data. Under the restrained dataset, the submission of a project proposal is required. After its review, based on relevance and feasibility, the proposal can be accepted and can be subjected to a maximum quota for product delivery. In principle, access is free of charge, upon accepting the ESA Terms and Conditions, but a contribution may be required. The restrained dataset includes SAR data from the ESA EO missions, as well as very large volumes of data due to their technical constraints. The ESA Data Policy applied to the ERS mission (1991-2011) which offered open and freely available data,[292] the Envisat mission (2002-2012) which offered open and freely available data,[293] and the Earth Explorer missions (2009-ongoing in 2022).[294] The data from these missions are available online through the ESA portal.[295]

The ESA Terms and Conditions for accessing EO data from its missions lay down further requirements for data use. According to them, ESA has the

289 The Rules specify further that information and data may take forms of technical data and technical assistance such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals, instructions, skills, training, working knowledge or consulting services, whether written or recorded on other media or devices such as disk, tape or read-only memories.

290 ESA Data Policy for ERS, Envisat and Earth Explorer missions (October 2012). For more on that policy, *see* G Suess, 'ESA Earth observation data policies: Principles, current status and reforms' in L J Smith, I Baumann, *Contracting for space – Contract practice in the European space sector* (Routledge, 2011) 405.

291 Terms and Conditions for the Utilisation of ESA's Earth Observation Data between the European Space Agency and the Principal Investigator, ESA-EOPG-PDGS-PR-1 (21 April 2020).

292 ERS mission description <https://earth.esa.int/eogateway/missions/ers>; ERS data <https://earth.esa.int/eogateway/missions/ers/data>.

293 Envisat mission description <https://earth.esa.int/eogateway/missions/envisat>; Envisat data <https://earth.esa.int/eogateway/missions/envisat/data>.

294 Earth Explorers mission description <https://www.esa.int/Applications/Observing_the_Earth/FutureEO/Earth_Explorers_ESA_s_pioneering_science_missions_for_Earth>.

295 ESA Earth observation gateway <https://earth.esa.int/eogateway/catalog>.

right to review, modify, suspend or terminate data delivery under certain conditions (B.3). Furthermore, ESA does not guarantee the suitability of the data for the desired purpose (A.2) and is not liable for damage derived by the use of the data, damage due to termination or suspension of data delivery, and damage due to malfunction or interruption of data delivery (A.3, B.8, B.9). The confidentiality of communications, reports and documentation involving this data is guaranteed only upon request and only if mutually agreed (A.4). Moreover, the data user acknowledges and takes into account scheduling and processing constraints on the ground and on board (B.2) and assumes full responsibility for data utilisation (B.4). The user should not assign any rights without authorisation (B.7) and should use the disclaimer 'Data provided by the European Space Agency' (B.13). ESA has the right to royalty-free publication and dissemination of user publications involving its data unless other limitations are in place (B.13). ESA has full title and ownership over these data (C.1). The user assumes such rights after interpreting the data (C.4), but should grant them to ESA free of charge, irrevocably and non-exclusively, for the purpose of space research and technology, if the interpretation was made using directly ESA data (C.5). These policies differ from the data policies for the Copernicus programme and the Galileo programme in which ESA participates.

The data policies of NASA govern the data, software, and publications that are part of its scientific research activities. The Science Mission Directorate Policy[296] applies to activities funded as part of the NASA missions. In principle, data are made publicly accessible, without a fee or restriction.[297] They should be machine-readable, include metadata, and be reusable with a clear, open, and accessible data license.[298] Exceptions may be in place for reasons related to intellectual property, export control, personal data, security, and the freedom of information. The data and information policy of the NASA Earth Science Program[299] governs the data collected by the programme's satellites.[300] These data should be shared fully and openly with all users as soon as they become available. The data products generated by NASA, their source code, coefficient, and ancillary data should also become available. Restrictions may apply subject to requirements from agreements with partners that provide data to the programme. Similar are the terms of the policy for

296 Science Mission Directorate Policy SMD Policy Document SPD-41 (4 August 2021) (hereinafter SMD Policy).

297 SMD Policy (n 296) art III.

298 According to the OPEN Government Act of 2018.

299 NASA Earth Science Program <https://science.nasa.gov/earth-science>. Data and Information Policy (updated 25 May 2021) <https://www.earthdata.nasa.gov/data-and-information-policy>.

300 NASA Earth System Observatory <https://science.nasa.gov/earth-science/earth-system-observatory>.

the data from the Earth Science Division, which should be openly available.[301] Data providers that are supported by NASA should implement the NASA data rights clause concerning algorithms and source code of open NASA data.[302] In particular, the clause protects the recipient's rights to data that embody trade secrets, as well as commercial, financial, or sensitive information, which may otherwise be open as part of NASA data. The protection comes in the form of exclusive access and use for two years to data that are first generated and processed by the recipient.

3.6.3 National data policies

National data policies are adopted by governments and govern the collection, access, use, and dissemination of space data from programmes that fall under their jurisdiction. Some national data policies, such as those in the US, Canada, France, and Germany, are part of regulations that concern the licensing of the space systems that collect space data. Other national data policies are stand-alone documents that concern specific datasets or general access to space data, such as in The Netherlands and India respectively.

– *Remote sensing in EU countries*

In *Germany*, the distribution of remote sensing data depends on whether they are high-grade data. Remote sensing activities are subject to the National Data Security Policy for Space-Based Earth Remote Sensing Systems,[303] which provides background information about the Act on Satellite Data Security.[304] The Act applies to German citizens and organisations falling under German law that are primary data distributors, excluding service providers, value-added service providers, and resellers. It covers space-based remote sensing systems of high-grade, depending on their spatial and spectral resolution, spectral coverage, and other system characteristics. The licensing procedure for these systems includes conditions regarding the distribution, but not the collection, of high-grade remote sensing data. According to this procedure, a data supplier conducts a sensitivity check on the data collected by the

301 Open data, services and software policies <https://www.earthdata.nasa.gov/engage/open-data-services-and-software>.

302 Data rights and related issues <https://www.earthdata.nasa.gov/engage/open-data-services-and-software/data-information-policy/data-rights-and-related-issues>.

303 National Data Security Policy for Space-Based Earth Remote Sensing Systems (2008) <https://www.bmwk.de/Redaktion/DE/Downloads/S-T/satdsig-hintergrund-en.pdf>.

304 Gesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten vor hochwertigen Erdfernerkundungsdaten (Satellitendatensicherheitsgesetz – SatDSiG), Zuletzt geändert durch Art. 5 G v. 19.4.2021 I 771 (hereinafter Satellite Data Security Act).

licensed system.[305] The sensitivity check involves the technical data of the sensors, the information included in the data based on the type of processing that is used, the surveyed area, the time of data acquisition and the time lag until the data supply, the requests of the data users, and the characteristics of the ground segment.[306] If the collected data is deemed sensitive, they should be reviewed by the competent authorities, that check the data distribution and metadata. Following the sensitivity check, an operator obtains a license to distribute high-grade remote sensing data. Moreover, the licensees are subject to government requests for priority access to data.

In *France*, the French Space Operations Act[307] lays down the licensing conditions for space activities under its scope.[308] The Act includes provisions specific to operators of space-based data, namely the natural or legal persons responsible for programming EO satellites or collecting EO data.[309] In particular, space data operators should declare their activities to the government and provide information regarding the characteristics of their system, including data resolution, geographic coverage, data accuracy, and observation band frequency.[310] Accordingly, the competent national authority decides whether the characteristics of the system can cause harm to national interests. For reasons of national interests and compliance with international obligations, that authority can impose at any time measures, including the suspension or delay of data distribution.[311] If the operator does not declare the required information or does not comply with the imposed measures, it can face fines.[312]

In *The Netherlands*, a data policy governs the use of space data that are made available through the Dutch Satellite Data Portal (Satellietdataportaal). The satellite data portal is an initiative of the Netherlands Space Office (NSO), to make satellite data available and promote their uptake. It consists of an online platform that offers access to satellite data of the territory of The Netherlands.[313] The data included in the portal are primarily EO data, which may

305 The Satellite Data Security Act (n 304) specifies that the sensitivity check is not conducted by the authorities, for reasons of efficiency and in order to promote commercialisation of remote sensing activities. The check relies on the distribution and the metadata.

306 Satellite Data Security Act (n 304) sec 15.

307 French Space Operations Act, LOI no.2008-518 du 3 Juin 2008 relative aux opérations spatiales, Journal Officiel de la République Francaise, 4 juin 2008. Translated into English in P Clerc and J Mariez, 'French Space Operations Act' (2008) 34 JSL 453 (hereinafter FSOA).

308 The FSOA (n 307) applies to operators in French national territory regardless of their nationality and to French operators abroad. More about its requirements and the licensing procedure can be found in B Lazare, 'The French Space Operations Act: Technical regulations' (2013) 92 Acta Astronautica 209, 210-211.

309 FSOA (n 307) art 1.7.

310 FSOA (n 307) art 23.

311 FSOA (n 307) art 24; P Achilleas, 'French remote sensing law' (2008) 34 JSL 1, 8-9.

312 FSOA (n 307) art 25.

313 Satellite Data Portal <https://www.satellietdataportaal.nl/>.

be fused with GNSS data and non-space data, such as aerial photography.[314] Optical EO data and radar EO data are provided in different resolutions, ranging from 30cm to 25m, in raw and processed format. Access to data is free of charge, but the use and processing of data from specific systems may be subject to conditions, as described in their respective license conditions.[315] At the time of this research, there are eight databases with license conditions included in the portal. Among their common conditions are the lack of warranties and liabilities, the compliance with IP laws, and the conditions to use the data. Concerning the latter, the uses are in principle divided between derivative works and value-added products. Derivative works usually refer to data and information that are compiled using the initial set of data, but where that initial set of data is no longer visible and cannot be uncoupled or reverse-engineered. Value-added products usually refer to data and information deriving from the initial set of data, which have been significantly altered or fused with other data, also unable to be uncoupled and reverse-engineered. Based on the license conditions, the use of derivative works and value-added products can be free, subject to accepting the license conditions of the initial dataset, limited to internal use, or prohibited. Along with the license conditions of the data suppliers, the Satellite Data Portal has a disclaimer that includes provisions regarding access to and use of its data.[316] According to the disclaimer, access to data is subject to accepting the license conditions in place. Additionally, the copyrights of the owners of the data should be respected, while the government does not accept liability for data accuracy and completeness.

– *Remote sensing in the USA, Canada, and India*

In the *US*, data policies are found in the Land Remote Sensing Policy Act[317] and the conditions regarding the licensing of private remote sensing activities by NOAA.[318] Unenhanced data from Landsat are owned by the US Government and should be made available to all users, in a timely and dependable manner, on a cost basis.[319] Other unenhanced data that are owned by the US Government should also be made available in a timely manner on terms that do not affect the commercial market for EO data.[320] Access to Landsat data and other US EO data is provided on a non-discriminatory basis, and

314 Available data <https://www.spaceoffice.nl/nl/satellietdataportaal/beschikbare-data/>.
315 Licensing requirements <https://www.spaceoffice.nl/nl/satellietdataportaal/toegang-data/licentievoorwaarden/>.
316 Disclaimer <spaceoffice.nl/nl/satellietdataportaal/disclaimer/>.
317 51 USC §601, 51 USC §60121.
318 15 CFR §960.
319 15 USC §60113.
320 15 USC §60132.

on grounds that respect national security interests.[321] Government and affiliated users may be entitled to a reduced price if they use the data for non-commercial purposes. Unenhanced EO data owned by the US Government and come from private satellites may be sold on the condition that they are not reproduced for commercial purposes.[322] The conditions for the licensing of a private remote sensing system apply to US operators and operators in the US.[323] The licensing terms depend on a tier-based approach based on the capabilities of the proposed remote sensing system.[324] Tier 1 concerns systems with the capabilities to collect unenhanced data of quality that is already available through systems that are not licensed by NOAA. Tier 2 concerns systems that produce unenhanced data substantially the same as already available data and Tier 3 concerns systems that produce unenhanced data that are not substantially the same as already available data. Data from systems in all tiers concerning the territory of a State should be made available to that State, upon request, on a reasonable cost basis.[325] Systems in Tier 2 and Tier 3 may be subject to government requests to limit data acquisition or dissemination for a given period, for reasons of national security and international obligations of the US.[326] Moreover, they may be required to provide a higher level of data encryption and unauthorised access protection.[327] Systems in Tier 3 can be subject to additional conditions when there is a specific and compelling risk that can be effectively addressed only through the conditions imposed on that system.[328]

In *Canada*, remote sensing is governed by the Remote Sensing Space Systems Act of 2005[329] and the Remote Sensing Space Systems Regulations.[330] The Remote Sensing Space Systems Act prescribes the licensing terms for the operation of remote sensing satellite systems that collect EO data. It covers the operation of the satellites, as well as the storage, processing, and dissemination of raw data from these satellites. Regarding the dissemination of data, Article 8.4 of the Act, lays down the conditions for obtaining a license

321 15 USC §60141.
322 15 USC §60143.
323 15 CFR §960.2.
324 15 CFR §960.6.
325 15 CFR §960.8.
326 15 CFR §960.9(a) and 960.10(a).
327 15 CFR §960.9(a.1) and 960.10(a.1).
328 15 CFR §960.10(d). NOAA, the licensing authority, has removed several conditions. J Foust, 'NOAA lifts many commercial remote sensing license conditions' (*Space News*, 8 August 2023)<https://spacenews.com/noaa-lifts-many-commercial-remote-sensing-license-conditions/>.
329 Remote Sensing Space Systems Act, S.C. 2005, c. 45 (last amended on April 5, 2007) (hereinafter Remote Sensing Space Systems Act).
330 Remote Sensing Space Systems Regulations, SOR/2007-66 (last amended on April 5, 2007) (hereinafter Remote Sensing Space Systems Regulations).

that include among others the supply of raw data and remote sensing products[331] concerning the territory of another country to that country's government upon request.[332] Article 8.6 of the Act describes the conditions that apply to the distribution of raw data upon the request of the competent Minister, namely the Minister of Foreign Affairs.[333] Raw data may be shared with others subject to the Minister's prior approval or under a legally enforceable agreement.

As far as remote sensing products are concerned, according to Article 8.7, the Minister may restrict their provisions on conditions that the Minister considers appropriate, namely the Minister's prior approval and a legally enforceable agreement. Moreover, the Minister can order priority access to any service on the grounds of international relations and obligations of Canada, according to Article 15.1. The Minister of Defence can request access to services on the grounds of Canada's defence and the safety of Canadian Forces, per Article 15.2. Similarly, the Minister of Public Safety and Emergency Preparedness can request access to services for the Police, the Security Intelligence Service, and for the protection of critical infrastructure and emergency preparedness, per Article 15.3.

Regarding the collection of data, Article 14 of the Act foresees interruption or restriction of service, for a specified period, on two occasions. First, if the Minister of Foreign Affairs orders it on the grounds of international relations and obligations of Canada. Second, if the Minister of Defence orders it on the grounds of Canada's defence and the safety of Canadian Forces. The Remote Sensing Space Systems Regulations were adopted pursuant to Article 20 of the Remote Sensing Space Systems Act, which provides for additional regulations on the recommendation of the Minister. They include provisions regarding the protection of data generated by the licensed systems, such as a command protection plan, notification of unauthorised data communication or security breaches, and maintenance of records and sales orders.[334]

In *India*, the Remote Sensing Data Policy of 2011[335] governs the acquisition and distribution of remote sensing data by non-government users that are acquired by Indian or foreign satellites. The Indian Space Research Organisation (ISRO) acquires and disseminates data from domestic and foreign

331 Raw data are defined as sensor data from EO satellites and any auxiliary data required to produce remote sensing products from the sensor data. Remote sensing products are also defined, as images or data produced from raw data in any way that transform the raw data. Remote Sensing Space Systems Act (n 329) art 2.

332 The supply of data to foreign governments does not extend to value-added data and products.

333 Remote Sensing Space Systems Act (n 329) art 2.

334 Remote Sensing Space Systems Regulations (n 330) art 1, 12, 15, and 16 respectively.

335 Remote Sensing Data Policy (2011) More about the regulation of remote sensing in India can be found in N Sarin, V Longani, 'The space law review: India' in J Wheeler (ed), *The Space Law Review*, (Law Business Research Ltd. 2020) 64.

sources. As far as domestic data are concerned, data collected by the Indian Remote Sensing programme (IRS) are solely and exclusively owned by the Indian Government. Interested parties can acquire a license for the use and added value of IRS data. Commercial entities are required to obtain a license to operate remote sensing satellites. As far as foreign data are concerned, the National Remote Sensing Centre[336] and Antrix Corporation Limited[337] are authorised to agree with foreign operators for the acquisition and distribution of foreign EO data in India. The acquisition of data depends on their resolution. Remote sensing data with a resolution of up to 1m are made available upon request on a non-discriminatory basis. Remote sensing data with a resolution higher than 1m are subject to clearance from the HR Image Clearance Committee. Such clearance is not required for government entities and commercial companies recommended by the government. For the acquisition and distribution of data, specific non-disclosure agreements should be signed with the National Remote Sensing Centre. The data policy of India is an example of a centralised system of data acquisition and distribution, whereby data by national and foreign satellites are gathered by a public authority that determines their distribution and use.

3.6.4 The UN Remote Sensing Principles

Remote sensing has been identified as one of the sources of space big data and currently provides the largest part of data, namely data in the form of images of the Earth from outer space. It also constitutes the most active field of space data and applications in terms of commercial growth and market development.[338] Therefore, it is worth addressing the Principles Relating to Remote Sensing of the Earth from Space (UN Remote Sensing Principles) that were adopted by the UN General Assembly, following the proposal of UNCOPUOS.[339] The UN Remote Sensing Principles do not have a binding legal effect, since they were adopted as a Resolution of the UN General Assembly and not as a treaty. They form part of 'soft law', namely guidelines that

336 National Remote Sensing Centre <https://www.nrsc.gov.in/>.
337 Antrix <https://www.antrix.co.in/>.
338 (n 205).
339 UNGA Res 41/65 (3 December 1986) Principles Relating to Remote Sensing of the Earth from Outer Space UN Doc A/RES/41/65 (hereinafter UN Remote Sensing Principles). C Q Christol, 'Remote sensing and international law' (1980) 5 Annals of Air and Space Law 375, 376; E Galloway, 'Present status of remote sensing in the United Nations' in M D Schwartz (ed), *Proceedings of the twentieth colloquium on the law of outer space* (Rothman Co 1978) 449.

express legal or political statements but are not agreed as binding text.[340] They are examined because they represent to date the sole international law document dedicated to space data in the form of imagery gathered using remote sensing of the Earth from outer space. The Principles are general and do not include specific obligations in the conduct of remote sensing.[341] Given that they were introduced over three decades ago, their content does not fully represent the current state of remote sensing technology and uses, which have evolved significantly ever since.[342] Nevertheless, they establish guidelines for the conduct of remote sensing activities, particularly concerning the freedom to conduct remote sensing, cooperation among States, and access to remote sensing data, which can find application in the current landscape.

– *Definitions and general provisions*

Principle I paragraph (a) provides the working definitions, which are used throughout the Resolution. Remote sensing is defined as the 'sensing of the Earth's surface from space by making use of the properties of electromagnetic waves'. This refers to specific remote sensing technology, namely the one that is based on the emission, reflection, or diffraction of electromagnetic waves by the sensed object. Remote sensing is further defined in Principle I as carried out for the improvement of natural resources management, land use, and the protection of the environment.[343] To this extent, the given definition and the scope of the Principles are limited compared to the existing uses of remote sensing satellites and remote sensing data, both in terms of the purpose of these uses and in terms of the technology deployed that may be more evolved

340 Gabrynowicz examines several criteria that are used to determine whether a document is seen as soft law, specifically in the context of the UN Remote Sensing Principles. She concludes that a determination regarding their soft law status should be seen in conjunction with the subject of the Principles and whether it has the potential to develop into a binding agreement. J I Gabrynowicz, 'The UN principles relating to remote sensing of the Earth from outer space and soft law' in I Marboe (ed), *Soft law in outer space – The function of non-binding norms in international space law* (Böhlau Verlag Wien 2012) 185-189 and 192-193.

341 H DeSaussure, 'Remote sensing: The interaction of domestic and international law' in *Proceedings of the Thirtieth Colloquium on the Law of Outer Space* (AIAA 1988) 295.

342 For more on the changes in the remote sensing landscape, involving evolving policies, increase in the number of sensing States, commercialisation and privatisation, and global cooperation, *see* M Hofmann, 'International legal framework of remote sensing in the year 2005: Changed conditions and changed needs', *Proceedings of the forty-eighth colloquium on the law of outer space* (AIAA 2006) 498-505.

343 For more about the meaning of 'environment' and 'natural resources' in the scope of the UN Remote Sensing Principles, *see* V D Bordunov, 'Remote sensing of Earth and its environment', *Proceedings of the twenty-third colloquium on the law of outer space* (AIAA 1981) 2.

than electromagnetic waves. Furthermore, the definition seems to be left out of the scope of the Principles of any commercial remote sensing activity.[344]

Principle I also defines the different categories of remote sensing data, which are respectively divided into 'primary data', 'processed data', and 'analysed information'. According to Principle I paragraph (b) primary data refer to raw data acquired by remote sensors borne by a space object, transmitted or delivered to the ground.[345] The transmission or delivery is performed by means of telemetry in the form of electromagnetic signals, photographic film, magnetic tape, or any other means. Processed data are defined in paragraph (c) as the products resulting from the processing of the primary data, in order to make the latter usable, while analysed information is defined in paragraph (d) as the information from the interpretation of processed data, inputs of data, and knowledge from other sources. Despite the narrower definition of remote sensing, the definitions of the various data categories encompass a much wider field of activities, especially since they extend to the processing of data.[346] These definitions could be used as a reference regarding the distinction among various levels of information included in remote sensing data, which could by extension be applied to other types of space data.

Apart from the definitions, the UN Remote Sensing Principles include general provisions related to compliance with international law (Principle III) and the responsibility of States for their national activities (Principle XIV). These provisions mirror Article III OST and Article VI OST respectively.[347] Another general guideline is included in Principle IX, according to which a State shall inform the UN Secretary-General about its remote sensing programme, pursuant to Article IV REG and Article XI OST. It should also make

344 During the drafting of the UN Remote Sensing Principles, the commercial aspects of remote sensing were not addressed due to lack of political will to proceed with such regulation. S Maureen-Williams, 'Reflections and suggestions on remote sensing and international law' (2001) 50 ZLW 409, 409 and 413-414.

345 A further distinction among primary data is suggested in V D Bordunov, 'Some legal problems of remote sensing of Earth from outer space' in M D Schwartz (ed), *Proceedings of the twentieth colloquium on the law of outer space* (Rothman and Co 1978) 497. The author distinguishes between global or regional data and local data, based on the 'spatial permission on the spot', so as to support that the former benefit every State and should be freely distributed, whereas as the dissemination of the latter should require the consent of the sensed State.

346 More on the definition of primary data, processed data, and analysed information in the scope of the UN Remote Sensing Principles can be found in V Kopal, 'Principles relating to remote sensing of the Earth from outer space: A significant outcome of international cooperation in the progressive development of space law' in *Proceedings of the thirtieth Colloquium on the Law of Outer Space* (AIAA 1988) 324.

347 UN Remote Sensing Principles (n 339) princ III and XIV do not add anything new, compared to the provisions of the OST. V Vereshchetin, V M Postyshev, 'Responsibility of states for remote sensing activities' in *Proceedings of the twenty-eighth Colloquium on the Law of Outer Space* (AIAA 1986) 247.

available to the greatest extent feasible and practicable, upon request, any information regarding its remote sensing activities for other States that might be affected by it. Finally, Principle XV calls for the resolution of any dispute stemming from the application of the Remote Sensing Principles amicably, according to the established procedures for peaceful settlement. Overall, these general principles refer to issues that are already addressed in the space treaties, which are binding to the States that have signed and ratified them. In this regard, the provisions of the space treaties would in any case apply to remote sensing activities, since the latter are a type of space activities that the space treaties govern. However, the UN Remote Sensing Principles tailor the general principles of the space treaties to the specific context of remote sensing and suggest that their application is particularly pertinent to this field of activities.

– *Sharing of benefits from remote sensing activities and cooperation among States*

The UN Remote Sensing Principles include several provisions about the benefits of remote sensing and the cooperation among States in materialising and sharing them. As explained in section 2.1.3, remote sensing activities offer several social, scientific, and economic benefits. According to Principle II, States conducting remote sensing activities should take into account the benefit and interest of all countries, irrespective of their degree of development, and should pay particular attention to the needs of developing countries, reinstating the equivalent provision of Article I OST. Open access to remote sensing data, as well as their offer under favourable conditions, make remote sensing activities accessible and fulfil the aim of this Principle. Similarly, cooperative schemes among countries and entities engage stakeholders with various levels of capability in remote sensing activities. The provisions of Principle II could be further strengthened by increased awareness regarding the benefits of remote sensing activities in which countries can partake.

As far as cooperation is concerned, Principle V includes a general statement on international cooperation among States in remote sensing activities, through making available opportunities for participation on equitable and mutually agreed terms. Although this provision does not seem to add significant substance to the Principles, especially given the aforementioned general rules, it serves to highlight the importance of cooperation in remote sensing and contextualising the cooperation among States that is mentioned in other Principles.[348] Principle VI suggests agreements as means of cooperation, to enhance the benefits derived from remote sensing activities. According to Principle VI, states are encouraged to collaborate in the data collection, storage,

348 V Kopal (n 346) 323-324.

process, and analysis, through the establishment of appropriate facilities. Technical assistance on the basis of mutual agreement by States with remote sensing activity is also envisioned in Principle VII, while Principle VIII involves the UN system in the promotion of international cooperation in remote sensing activities. Finally, Principle XIII calls for the promotion and intensification of international cooperation, as well as for States to enter, upon request, into consultations with other States whose territory is sensed, to create opportunities for participation and enhancement of benefits. Given the above, the UN Remote Sensing Principles go beyond the scope of the Outer Space Treaty and include actionable means of cooperation among countries.

– *Access to remote sensing data and the right to sensed and sensing States*

The UN Remote Sensing Principles establish two fundamental premises for the conduct of remote sensing activities. First, the sensing State can lawfully conduct remote sensing without the consent of the sensed State. Second, the sensed State has, under conditions access to data concerning its territory.

As far as the lawful conduct of remote sensing is concerned, Principle IV reinstates the fundamental space law principle mentioned in Article I OST, namely the freedom of exploration and use of outer space.[349] Principle IV goes on to emphasise the respect of the sovereignty of all States and peoples over their territory and natural wealth and the due regard to the interest of other States and entities, under which remote sensing activities should be carried out. Accordingly, remote sensing should not be conducted in a manner detrimental to the legitimate rights and interests of the sensed State. This provision is the outcome of the debate over the legality of remote sensing, which stemmed from the conundrum between the freedom of remote sensing as a space activity and the collection of information about a State's territory by remote sensing.[350] This debate reflected the circumstances at the time of the adoption of the Principles when remote sensing was a new activity that was perceived as means of surveillance of the territory of another State for national or defence purposes or for monitoring natural resources. Therefore, the issue of the sovereignty of States was brought up by several countries that

349 Gorove questions whether, according to Article I OST, the exploration of outer space should precede its use or whether the use should accompany the exploration, since the text of the Article mentions exploration *and* use, rather than exploration *or* use. He connects this question to remote sensing by further questioning whether Article I OST would find application in remote sensing activities that use outer space, but do not explore it and concludes that remote sensing mainly explores the Earth. In S Gorove, 'Earth resources satellites and international law' (1973) 1 JSL 80, 81.

350 A Ito, *Legal aspects of remote sensing* (Studies in Space Law vol 5, Brill 2011) 46-47; R F Stowe, 'The development of international law relating to remote sensing of the Earth from outer space' (1977) 5 JSL 101, 106; A A Cocca, 'Remote sensing of natural resources by means of space technology: A Latin American point of view' in M Matte, H DeSaussure (eds), *Legal implications of remote sensing from outer space* (Sijthoff 1976) 66-67.

feared that their natural wealth was exposed to the sensing State or any other State that acquired remote sensing information. During the negotiations preceding the adoption of the UN Remote Sensing Principles, States expressed several different and often conflicting opinions on the practice of remote sensing.

Despite the expressed concerns, the UN Remote Sensing Principles do not require any form of consent or agreement of the sensed State for its territory to be monitored by the sensing State.[351] Moreover, remote sensing can be lawfully carried out as an embodiment of the freedom to use and explore outer space of Article I OST.[352]

Some of the concerns around the freedom of the sensing States were offset by the principles regarding access of the sensed State to data concerning its territory. In particular, Principle XII establishes the right of the sensed State to obtain access to data concerning the territory under its jurisdiction on a non-discriminatory basis. The access of the sensed State includes both primary and processed data, as well as analysed information.

In addition to the provisions regarding access to the sensed State, the UN Remote Sensing Principles provide for dissemination of remote sensing data for specific cases. As mentioned, the purpose of remote sensing described in Principle I is to improve natural resources management and land use and to protect the environment. Principle X provides for sharing information capable of averting phenomena harmful to the Earth's environment with concerned States. Similarly, Principle XI calls for States possessing information regarding natural disasters to share it as soon as possible with States that are affected or likely to be affected. Despite their specific scope, Principles X and XI affirm that remote sensing data should be on occasion openly accessible, thanks to the significance of the information they entail.

351 S Mosteshar, 'Regulation of remote sensing by satellites' in R Jakhu, P S Dempsey (eds), *Routledge handbook on space law* (Routledge 2016) 151; D Zannoni, *Disaster management and international space law* (Studies in Space Law vol 15, Brill 2019) 167-168; C Q Christol, '1986 Remote Sensing Principles: Emerging or existing law' in *Proceedings of the thirtieth Colloquium on the Law of Outer Space* (AIAA 1988) 272; R Jakhu, 'International policy and law-making process for remote sensing by satellite' (1998) 22 Annals of Air and Space Law 451, 452.

352 G P Zhukov, 'Problems of legal regulation of using information concerning remote sensing of the Earth from space' in M Matte, H DeSaussure (eds), *Legal implications of remote sensing from outer space* (Sijthoff 1976) 127; C Q Christol (n 339), 392; S Gorove, 'International legal aspects of Earth resources satellites in M D Schwartz, *Proceedings of the fiftieth colloquium on the law of outer space* (Rothman and Co 1973) 30. *See* also the analysis on Article I OST in the context of space big data in section 3.1.1 and the legal challenge related to the collection of information about States via satellite in section 4.2.

3.6.5 Preliminary conclusions on the connection between data policies and space big data

Data policies govern data from specific programmes, such as the EU Copernicus, or data suppliers in specific jurisdictions, as is the case with national data policies. They influence space big data since they impose requirements concerning the access to, use, and dissemination of data.

Data policies partly stem from the obligations of States as parties to the international space treaties, as elaborated in section 3.1.1. They also serve the interests of States and organisations that have adopted such policies, in terms of promoting their data and safeguarding national security. The policies of the EU Space Programme extend to most space data categories and include provisions related to EO data, satellite-enabled location data, space-based connectivity data, and SSA data in the framework of the programme. The data policies of space agencies and national data policies mainly concern EO data. Likewise, the UN Remote Sensing Principles can also serve as a general basis for EO data policies.

3.7 Chapter conclusion

This chapter addressed research question 2 "what are current laws and data policies applicable to space big data based on the type of data and data uses?". The applicable laws include international space law, privacy and data protection law, intellectual property law, cybersecurity law, export control, and data policies related to space data. These are the most relevant laws and data policies applicable to space big data because they affect the collection, access, use, and dissemination of space big data and these parameters are important for maintaining and enhancing the benefits from space big data, as described in chapter 2. These laws apply to space big data, but also apply to the satellites involved in the space big data lifecycle and the information that space big data contain. The data policies are relevant because they govern specific categories of space data. Each legal field affects different stages of the space big data lifecycle. Except for the relevant conclusions in the following paragraphs of this section, the impact of each legal field is further discussed in chapter 4, in conjunction with the impact of the legal challenges connected to each field, and is summarised in table 4.2 in section 4.8.

First, international space law applies to space big data because the satellites that collect, store, and transmit space big data fall under its scope. Several provisions of the UN Space Treaties find application. Article I of the Outer Space Treaty (OST) establishes the freedom to use and explore outer space, which includes the freedom to launch satellites involved in the space big data lifecycle. It also calls upon States to conduct space activities for the benefit and in the interest of humankind. Space big data materialise the benefit-sharing

principle thanks to their availability and the variety of social and economic purposes they can serve. Article II OST declares outer space as an area outside national sovereignty and raises challenges with regard to the laws applicable to the part of the space big data lifecycle that takes place in outer space. Article VI OST concerning the international responsibility of States for the activities of their nationals in outer space creates a connection between satellites involved in space big data and States that authorise and supervise them. Article VII OST, along with the provisions of the Liability Convention, establishes international liability for the launching State for damages on the Earth and in outer space, which is relevant when damages are caused to or by a satellite collecting or transmitting space big data. Article VIII OST and the provisions of the Registration Convention provide for jurisdiction and control over registered satellites that are involved in space big data, thus creating a link between States and objects found in outer space. Finally, Article IX OST calls for States to consult, to avoid potentially harmful interference with the activities of other States, which may disrupt the flow of space big data. Similarly, the framework of the International Telecommunication Union (ITU) provides for the allocation of radiofrequency and orbital spectrum and establishes measures for avoiding harmful interference. Space law influences the collection, access, use, and dissemination of space big data.

Second, privacy and data protection are relevant to the space big data that identify or can identify individuals, when used separately or in combination with other available data, both space and non-space. They especially impact the collection, use, and dissemination of data. According to the EU data protection framework, the controllers and processors of personal data should follow requirements concerning the lawful collection and processing of these data.

Third, intellectual property rights are attached to datasets, processed data, data products, and technologies deployed in the space big data lifecycle. They protect the rights of the creators or owners of an intellectual product and can limit or condition the access, use, and dissemination of space big data.

Fourth, cybersecurity regulations protect the space-based and ground-based segments of the space big data lifecycle that rely on network and information systems. The actors involved in space big data that operate such systems should implement sufficient security standards. Cybersecurity is essential in the access, use, and dissemination of data.

Fifth, export regulations apply to space big data, since the technology used in data collection and processing, as well as datasets, may fall under lists of controlled items. Export control affects the collection, access, use, and dissemination of space big data.

Sixth, various data policies are applicable to space big data. The EU Space Programme entails the use of Global Navigation Satellite Systems (GNSS) data and space situational awareness (SSA) data for the operation of its components, Galileo, EGNOS, and SSA. It also involves the collection of big Earth Observa-

tion (EO) data by Copernicus and most recently the operation of a constellation providing secure satellite-based connectivity. Primarily, the EU Space Programme offers open and free access to data collected and used by its components. However, some types of data or data services may be limited to certain users or conditionally accessible, for reasons related to the security of the components and the type of the services they offer. Moreover, national data policies apply to space big data, particularly EO data collected by remote sensing systems licensed or operated in these jurisdictions. The UN Remote Sensing Principles, albeit non-binding, introduce basic guidelines for the conduct of remote sensing activities, including the lawfulness of remote sensing without the consent of the sensed State, the access of the sensed State to data concerning its territory on a non-discriminatory basis, and the sharing of remote sensing data to prevent environmental and natural disasters. Data policies specific to systems that collect space big data are also applicable. Data policies can impact the collection, access, use, and dissemination of data.

An overview of the examined laws and data policies, their relevance to space big data, and the type of space data they affect can be seen in table 3.1.

Table 3.1 – Overview of the laws and data policies relevant to space big data and the type of space data they affect

Space (big) data reference	Relevance to space (big) data	Type of space data affected
International space law		
No	International space law regulates the satellite systems that collect and transmit space (big) data, which should comply with their provisions.	- EO - GNSS - space-based connectivity - astronomy and others
Impact on the space big data lifecycle: collection, access, use, dissemination		
Privacy and data protection law		
Indirectly (location data and high-resolution EO data that can identify individuals)	If personal data are collected or processed in the course of space (big) data activities, the data controller, the data processor, and the data subject should be identified and the requirements for the lawful collection and processing of personal data should be fulfilled.	- EO - GNSS - space-based connectivity
Impact on the space big data lifecycle: collection, use, dissemination		
Intellectual property law		
No	IP laws may limit or impose conditions to the access, use, and dissemination of space (big) data. They determine which data and databases are copyrighted and which patented technologies used in space (big) data processing are protected.	- EO - GNSS - space-based connectivity - astronomy and others
Impact on the space big data lifecycle: access, use, dissemination		
Cybersecurity law		
Yes (network and information systems)	Cybersecurity laws apply to satellite systems under their scope that provide space (big) data flow, as well as to stored space (big) data. They provide for the adoption of cybersecurity measures and the response to cyber incidents.	- EO - GNSS - space-based connectivity - astronomy and others
Impact on the space big data lifecycle: access, use, dissemination		
Export control		
No	Export control laws may apply to dual-use space (big) data and to technology, such as satellite sensors, that is used to collect and process space (big) data. They may also limit the export of controlled items, in cases of data access by foreign users and for certain purposes.	- EO - GNSS - space-based connectivity - astronomy and others
Impact on the space big data lifecycle: collection, access, use, dissemination		
Data policies		
Yes (EO data, GNSS data, space-based connectivity data, SSA data)	Data policies govern specific categories of space data and include provisions regarding the licensing of space systems that collect space data or the terms of data access and use.	- EO - GNSS - space-based connectivity - astronomy and others
Impact on the space big data lifecycle: collection, access, use, dissemination		

The laws and data policies that are examined in this chapter apply to space big data, regardless of whether they strictly fall under the definition of space data or big data. Even when space data are combined with non-space data or when they are further reused and processed outside the space big data lifecycle, the same legal issues are applicable. Even when space data do not qualify as big data, the described legal aspects are relevant. The elements of big data determine the efficiency and not the applicability of relevant laws and data policies. The only parameter that impacts the applicability of these laws and policies is whether parts of the space big data lifecycle take part in outer space. Due to the lack of national sovereignty in outer space, unless these laws and policies include the space-based part of the lifecycle in their scope, they may not find application.

Having identified the laws and data policies relevant to space big data, chapter 4 will assess how they apply to space big data and applications.