Izzo L, 'Satellite Data Management and Privacy Law' (2024) 1 EJPLT, 219-230.
DOI: https://doi.org/10.57230/EJPLT241LI

EJPLT
ISSN 2704-8012



EO Satellite Data Management and Privacy Law*

La gestione dei dati satellitari nell'osservazione della Terra e la tutela della privacy

Luigi Izzo
Ph.D.(s) in Humanities and Technologies: an integrated research path
Università degli Studi Suor Orsola Benincasa

Abstract

The relevance of the space sector is increasing, with reference not only to the traditional telecommunications satellites but also to Earth Observation satellites, equipped with increasingly sophisticated electro-optical, radar and spectrographic payloads capable of collecting increasingly precise and well-defined data. This space race sees the participation above all of private entities that carry out extensive data collection, with the sole aim of making it profitable. In this light, the aim of the paper is to specifically analyze the issue of personal data processing, also with regard to the latest advances in the field of sensors and access to space.

La rilevanza del settore spaziale sta aumentando, con riferimento non solo ai tradizionali satelliti per le telecomunicazioni ma anche quelli per l'Osservazione della Terra, dotati di payload elettro-ottici, radar e spettrografici sempre più sofisticati e in grado di raccogliere dati sempre più precisi e definiti. Questa corsa allo spazio vede la partecipazione soprattutto di soggetti privati che effettuano un'ampia raccolta di dati, con l'unico scopo di renderla redditizia. In quest'ottica, l'obiettivo del documento è quello di analizzare nello specifico la questione del trattamento dei dati personali, anche in relazione agli ultimi progressi nel campo dei sensori e dell'accesso allo spazio.

* The paper is the result of the work of a researcher of the Research Centre of European Private Law (ReCEPL) at Università degli Studi Suor Orsola Benincasa, with the collaboration of PhD(s) Alessandra Fabrocini and PhD Anna Anita Mollo, and the coordination of the ReCEPL Director Prof. Lucilla Gatt and the ReCEPL Vice-Director Prof. Ilaria A. Caggiano.
The work was presented at the IEEE International Conference 'MetroAeroSpace', held in the Bovisa Campus, Politecnico di Milano, Milan, June 19-21, 2023, and published in the 2023 IEEE 10th International Workshop on Metrology for AeroSpace (MetroAeroSpace), 247.

Image: ESA/ATG medialab

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Earth Observation; Satellite Data; Data Management; Privacy Law.

Summary: 1. Introduction. – 2. The international framework on space activities. – 3. National and EU laws on remote sensing activities. – 3.1. Lobbying in the field of EO operations. – 3.2. Some example of national frameworks. – 3.3. EU framework for remote sensing activities: the Copernicus Programme. – 4. A combination of licensing procedures with privacy assessment? – 4.1. When can EO data become personal data? – 4.2. A first hypothesis: combining evaluation for ITU licences with privacy protection. – 5. Conclusions.

1. Introduction.

The Space Age, which in fact began as a result of Wernher von Braun's rocket research, saw as its protagonists the States. However, it is also true that the private sector immediately experienced intensive growth, which began in the United States of America with telecommunications satellites (Communications Satellite Act of 1962) and later extended to almost every type of space activity (Commercial Space Launch Act of 1984). Subsequently, the various national regulations have evolved steadily to encompass all areas of space operations and to bolster the competitiveness of companies operating in the overall sector.

This has allowed private players to attract new investments, further advancing technologies and reducing the cost of the assets needed to operate in the space[1]. This is true not only in the field of telecommunications or geolocation but also in the field of Earth Observation.

First of all, the progressive process of miniaturisation of the electronic and sensor components in general of satellites must be considered. For example, SAR sensors - in the civil sector - were initially used on a platform whose mass was 1800 kg (NASA SeaSat 1, launched in 1978[2]) while we are now witnessing a miniaturisation such that they can be used on platforms in the 'smallsat' class[3] and on specific microsatellites[4], in contrast to the large platforms still used by States[5].

The same tendency is also present for optical sensors, already available for CUBESat satellites[6]. Another element to be taken into account is the wide availability of medium or light launchers for launching satellites, whose

[1] D. Chow, "To cheaply go: How falling launch costs fueled a thriving economy in orbit", https://www.nbcnews.com/, April 2022.
[2] NASA webpage for the SeaSat 1 satellite, https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=1978-064A
[3] FAA, The Annual Compendium of Commercial Space Transportation: 2018, 2018, p. 94.
[4] A. Golkar, G. Cataldo, K. Osipova, "Small satellite synthetic aperture radar (SAR) design: A trade space exploration model", Acta Astronautica, Vol. 187, 2021, 458-474. See also W. Johannes *et al.*, "Miniaturized high resolution Synthetic Aperture Radar at 94 GHz for microlite aircraft or UAV," SENSORS, 2011 IEEE, Limerick, Ireland, 2011, 2022-2025.
[5] S.W. Paek, S. Balasubramanian, S. Kim, O. de Weck, "Small-Satellite Synthetic Aperture Radar for Continuous Global Biospheric Monitoring: A Review.", Remote Sens. 2020, 12, 2546.
[6] T. Rotovnik, D. Gacnik, I. Kramberger, "Miniaturized Multispectral VNIR/SWIR Imager for Small Satellites - System Design", IFAC-PapersOnLine, Vol. 48, Issue 10, 2015, 12-15.

operating costs are much lower than those for 'heavy' launchers[7]. But, now, the launchers are being challenged by an even cheaper system, at least for the smallest satellites, a ground-based 'slingshot' designed by SpinLaunch[8], with a single launch cost of less than half a million dollars[9].

Finally, consider the advances in the field of image resolution. With reference only to SAR sensors, if we compare images produced in the 1990s with those currently available, we can see that in the 1990s the EO satellites were using a C-Band sensor with a resolution of 20m, while the satellites launched in the first decade of 2000s were using X-band sensors with a resolution of 1m[10]. Thus, in less than two decades, an outstanding achievement in the field of SAR sensors has been achieved, increasing the attractiveness of their data.

As a result of the above, new issues arise from a legal point of view. In the long run, it would be possible to perpetrate violations of the privacy of individuals through the processing of images from EO satellites. Of course, this might seem like a forced and hasty statement. Yet, as has happened in the fields of telecommunications, geo-localisation and information technology, nothing prevents technological advances and economic policy choices by major private players from leading to privacy risks.

Just with regard to information technology and personal computers, the initial spread of PCs and the Internet could not lead to systematic and widespread privacy concerns, which only spread later, with innovations in operating systems and economic policy choices[11], forcing legislators to address the issue and introduce new legal instruments. Thus, action was taken, but only after the problem had manifested itself, instead of adopting an overall approach aimed at preventing it, as far as possible.

2. The international framework on space activities.

First, it is worth taking a brief look at the international law framework on space.

As is well known, the *Corpus Iuris Spatialis* saw the light of day in a context of high conflict and its core consists of five Treaties: the Outer Space Treaty, the Rescue Agreement, the Liability Convention, the Registration Convention and the Moon Agreement[12], all drafted by the Committee on the Peaceful Uses of

[7] See FAA, The Annual Compendium, Launch Vehicle Fact Sheets "Falcon 9" and "Vega". See also J. Joly, "Move over, SpaceX: ArianeGroup to make Europe's first reusable and 'eco-friendly' rockets", www.euronews.com, July 2022.
[8] SpinLaunch homepage, https://www.spinlaunch.com/
[9] P. V. Siddhart, "Why Launch Rockets When You Can Just Fling Them Into Space?", https://www.bloomberg.com/, May 2023.
[10] A. Moreira, P. Prats-Iraola, M. Younis, G. Krieger, I. Hajnsek, and K. Papathanassiou, A Tutorial on Synthetic Aperture Radar. IEEE Geoscience and Remote Sensing Magazine, vol. 1, issue 1, April 2013, 6-43.
[11] See L. Gatt, R. Montanari and I.A. Caggiano (eds.), Privacy and Consent. A Legal and UX&HMI Approach University Suor Orsola Press, 2021. L. Gatt (ed.), Social Networks and Multimedia Habitats. Jean Monnet Chair PROTECH. "European Protection Law of Individuals in Relation to New Technologies". 1st International Workshop A.Y. 2019-2020 University Suor Orsola Press, 2020.
[12] For more information about the Five Treaties see F. G. von der Dunk, Advanced Introduction to Space Law, Elgar, 2020, 14-39.

Outer Space (COPUOS) of the United Nations[13]. The 1967 Outer Space Treaty, actually considered *customary law*, contains the structural principles that regulate activities in outer space. This means that any space activity by any Nation is subject to the provisions of this Treaty.

However, it is focused on peaceful cooperation, on the impossibility of placing state jurisdictions in orbit (as is the case, instead, with the so-called 'territorial waters' and 'national airspace'). This is the reason why the first four articles (Articles I, II, III, IV) focus on conceptually denying the possibility of expanding national jurisdictions beyond their current boundaries. It follows, therefore, that the Treaty just referred to does not focus at all on the activities of private entities, even though, due to the provisions of Articles VI, VII and VIII and, above all, thanks to the existence of a convention on the registration of 'vehicles' sent into orbit, it constitutes the fundamental basis for any further development of space legislation. This is also due to the presence of provisions that are deliberately broad in meaning, so that they can be applied by interpretation in the most diverse cases, as well as serving as a legal basis for various future provisions. Indeed, it would not be wrong to think that the Outer Space Treaty is, in the sphere of space and international law, a kind of Constitutional Charter, from which all other provisions relevant to the sphere under consideration are derived.

This makes it possible to introduce UN General Assembly Resolution 41/65[14], which, as far as the subject of this contribution is concerned, still focuses on legal entities called 'States' but provides an initial legal basis for remote sensing activities. In fact, the resolution is headed 'Principles Relating to Remote Sensing of the Earth from Outer Space'. This resolution recalls the concept of peaceful exploitation of space based precisely on the provisions of the Outer Space Treaty (see Principle III).

The problem addressed by the Resolution was very simple: as F. G. von der Dunk summarises, it "*concerned the increasing possibilities of using satellite remote sensing for sounding out terrestrial opportunities for mineral resource mining […] giving rise to worries in particular with developing States being sensed that the developed State sensing them would use the knowledge gained for their own economic purposes, in addition to worries that data which could alleviate suffering and destruction in humanitarian crises would not be made readily and/or freely available*"[15]. For this reason, the sensed States sought to promote the principle of "prior consent" in the field of remote sensing while the States operating the satellites were obviously against such a regulatory development.

In an attempt to reconcile the two, Principle XII was outlined, which provides that the sensed State shall have access to these data on a non-discriminatory basis and on reasonable cost terms, taking particularly into account the needs and interests of the developing countries.

The problem is this: does the data that can be accessed also include data produced by private companies specialising in remote sensing (e.g. Maxar) or

[13] COPUOS webpage: https://www.unoosa.org/oosa/en/ourwork/copuos/index.html
[14] UN General Assembly Resolution 41/65 - https://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/remote-sensing-principles.html
[15] F. G. von der Dunk, Advanced Introduction to Space Law, 59.

only those produced by state-owned satellites[16]? If one considers that the principle requires that the data must be in the possession of the State carrying out the remote sensing activities, then it could be understood to mean that data in the possession of companies specialising in Earth Observation in that same State are not covered by this principle. Therefore, those companies would be free to sell them on the market at the conditions they consider most appropriate. If one thinks, however, that Principle XIV invokes the responsibility of States under Article VI of the Outer Space Treaty, then one might think that States with such responsibility are also, in a sense, 'in possession' of the data generated by private operators authorised by them. Thus, data generated by private EO satellites would also be subject to the provisions of Principle XII. In both cases, since this was a UN Resolution passed in 1986, no consideration was given to the possibility that such data might later lead to hypothetical violations of privacy.

3. National and EU laws on remote sensing activities.

3.1. Lobbying in the field of EO operations.

First of all, when talking about EO activities and the respective national regulations, it is necessary to start from a fundamental element: these are legal provisions aimed at private legal entities and designed to reconcile the needs of the market with national security requirements. For this very reason, it is impossible to deny the existence of lobbying activity at the national level, in the various states with a flourishing aerospace industry, especially those in the West, aimed at reducing the limits on the resolution and dissemination of data produced by EO satellites[17].

This activity has become even more intense in recent years in view of the progress made by various states (India, China, etc.) in developing their aerospace industries [18]. Hence, a serious issue arose concerning the competitiveness of Western companies, influencing the evolution of national regulations.

3.2. Some examples of national frameworks.

First consider the US framework, placed in the Code of Federal Regulations, in the Title devoted to Foreign Trade (Title 15, Subtitle B, Chapter IX, Subchapter D, Part 960)[19], recently reformed involving the NOAA and the major players in the industry[20].

---

[16] F. G. von der Dunk, Advanced Introduction to Space Law, pp. 61 and following.

[17] P. B. de Selding, "Satellite Imagery Firms in U.S. and Europe Pushing for Permission To Sell Sharper Imagery", https://spacenews.co/, September 2013. T. Hicthens, "Commerce Slashes Restrictions On Remote Sensing Sats", https://breakingdefense.com/, May 2020.

[18] S. Singh, "New space policy allows pvt cos to set up, operate own network of remote sensing satellites", https://timesofindia.indiatimes.com/, April 2023.

[19] US Code of Federal Regulations, Title 15, Subtitle B, Chapter IX, Subchapter D, Part 960, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-IX/subchapter-D/part-960

[20] Comments to the Final Rule, https://www.regulations.gov/document/NOAA-NESDIS-2018-0058-0040/comment.

This has led to a licensing system based on three tiers, each characterised by a common set of operating conditions plus a set of peculiar predictions for each Tier. When analysing the characteristics of the various Tiers, it becomes clear that the first two concern licences for remote sensing systems operating in an internationally competitive environment. Conversely, Tier 3 is aimed at those companies that intend to provide products that do not currently exist on the market, as in the case of the 10cm resolution imagery promised by Albedo Space Corp[21].

The US system, therefore, is aimed above all at ensuring national security, protecting the competitiveness of domestic remote sensing companies only to the extent strictly necessary for this purpose, so much so that the various operators in the sector have not concealed a certain disappointment with the reformed regulations that have come into force[22]. Yet, as the case of Albedo shows, NOAA does not prevent such companies from obtaining licences to operate remote sensing systems with resolutions so high that they are not available from other competitors. However, if there are no national security reasons to note, there does not seem to be a mechanism to limit dissemination. So, the various companies could - one day - produce imagery with a resolution of 5cm relating to an urban area totally devoid of military targets (or national security agency facilities) and be able to sell it to anyone, without limits, precisely because there are no elements such as those mentioned above to limit its dissemination.

With regard to regulations in countries other than the US, examples include the Title VII Space Operations Act and its implementing legislation in France[23], the Satellite Data Security Act (SatDSiG) of 2007 and the Satellite Data Security Ordinance (SatDSiV) of 2008 in Germany[24].

First of all, the French framework has been implemented with additional regulatory outline provisions, specifically Decree 2009-640 of June 2009, the Order of 4 September 2013, and Decree 2013-654 of July 2013. A key feature is that, once resolution limits are outlined for satellite images, operators only have to notify the Secretariat General of Defence of the start of operations two months in advance if the payload installed on the satellites is such that it exceeds these limits. So, there are no *ex-ante* limitations. The Secretariat can only provide for *ex-post* limitations where necessary and only if the resolution limits provided for by the regulations are exceeded. Hence, if the sensors do not exceed these limits, they are not subject to the *ex-ante* reporting requirement, nor can they be subject to data dissemination limitations[25].

---

[21] D. Werner, "Albedo wins license to sell 10-centimeter imagery", December 2021, https://spacenews.com/

[22] For instance, see the comments of Maxar Technologies Inc., Capella Space Corp. and Planet Labs Inc. about alleged ambiguities in the regulatory dictate regarding the requirements for each specific Tier. They also rail against transparency obligations.

[23] Loi no 2008-518 du 3 juin 2008 relative aux operations spatiales, Republique Francaise, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000018931380.

[24] Satellitendatensicherheitsgesetz, vom 23. November 2007 (BGBl. I S. 2590), das zuletzt durch Artikel 92 des Gesetzes vom 29. M€ arz 2017 (BGBl. I S. 626), Bundesministerium der Justiz und Fur Verbraucherschut https://www.gesetze-im-internet.de/satdsig/index.html - Satellitendatensicherheitsverordnung, vom 26. Marz 2008 (BGBl. I S. 508), die durch Artikel 1 der Verordnung vom 30. Juli 2014 (BGBl. I S. 1314), Bundesministerium der Justiz und Fur Verbraucherschutz https://www.gesetze-im-internet.de/satdsiv/.

[25] R. Harris, I. Baumann, "Satellite Earth Observation and National Data Regulation", Space Policy, 56, 2021, 3.

In Germany, however, an approach based entirely on primary legislation seems to predominate. The SatDSiG is the basic law, while the SatDSiV contains the technical characteristics used to classify Earth observation data as sensitive or non-sensitive. This regulation focuses, unlike the French one, not only on the resolution limits, but also on certain aspects of data dissemination, mainly related to assessing the reliability of the data requester and whether these data concern sensitive areas for national security[26]. The sensitivity check procedure is already outlined in the SatDSiG.

However, as in the case of the US framework, the French and German frameworks do not adopt privacy risk assessment procedures, limiting themselves solely to protecting national security.

3.3. EU framework for remote sensing activities: the Copernicus Programme.

Given the above, it is possible to analyse European legislation on Earth observation operations. However, in order to better understand the current European regulatory framework, it is necessary to reconstruct its evolution.

It all started in 1998 with the establishment of the GMES Programme (subsequently named Copernicus Programme), an Earth monitoring initiative led by the Union and implemented in cooperation with the Member States and the European Space Agency (ESA). Its objective, since the time of the Baveno Manifesto[27], has been to provide, under the control of the Union, information services that allow access to accurate data and information in the field of environment and security, adapted to the needs of users. Subsequently, the GMES programme was formally established by Regulation (EU) No 911/2010[28], which immediately paid attention (albeit with brief references) to the protection of personal data. In Recital 27, in fact, the European legislator expresses itself in these words: "*GMES initial operations should be implemented consistently with other relevant Union policies, instruments and action, in particular with […] the protection of personal data.*". Article 4(2) also states that "*The Commission shall manage the funds allocated to the activities under this Regulation in accordance with the Financial Regulation and with the management procedure referred to in Article 16(4). It shall ensure the complementarity and consistency of the GMES programme with other relevant Union policies, instruments and actions, relating in particular to the […], the protection of personal data […]*".

This led to the issuing of the Commission Delegated Regulation (EU) No 1159/2013[29], drafted in order to establish registration and licensing conditions for GMES users and define criteria for restricting access to GMES dedicated data and GMES service information. Recital 12 of this Delegated Regulation follows what was already described in recital 27 of the 2010 Regulation. Even

[26] R. Harris, I. Baumann, "Satellite Earth Observation and National Data Regulation" 4.
[27] Editorial, "A short history of the Copernicus In Situ Component since the Baveno Manifesto", June 2018, https://insitu.copernicus.eu/news/the-copernicus-in-situ-component-since-the-baveno-manifesto.
[28] Regulation (EU) No 911/2010 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32010R0911.
[29] Commission Delegated Regulation (EU) No 1159/2013 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R1159.

more important is the content of the Regulation itself, since it makes a very clear separation between the protection of the national security of European countries and the protection of the privacy of individuals. While national security is the subject of Art. 12, privacy is included among the conflicting rights listed (non-exhaustively) in Art. 11, always leaving it to the Commission to act, on a case-by-case basis and if necessary, to limit the dissemination of EO data.

As can be seen on the official EUR-Lex website, this Delegated Regulation is still in force, despite the fact that the 2010 Regulation was repealed by Regulation (EU) No 377/2014[30], which only mentions the protection of personal data in Recital 9, along the lines of what was written in Recital 27 of the repealed Regulation. Subsequently, the 2014 Regulation was in turn repealed by Regulation (EU) 2021/696[31], which created a European Union Space Agency (EUSPA, not to be confused with its partner ESA, the European Space Agency, founded several decades earlier) and provided the legal basis for a fully-fledged European space programme, including the Copernicus programme.

This Regulation fully takes up the legacy of the previous regulatory texts. In fact, in Recital 81 it expressly recalls the 2013 Delegated Regulation, requiring its application and compliance, and there is a dedicated article, Article 104(1), aimed precisely at the protection of personal data which states as follows: *'1. All personal data handled in the context of the tasks and activities provided for in this Regulation, including by the Agency, shall be processed in accordance with the applicable law on personal data protection, in particular Regulations (EU) 2016/679 and (EU) 2018/1725 of the European Parliament and of the Council.*'.

As can be seen, the expression is particularly broad (which makes its application by interpretation possible even in future and particularly problematic cases) and such as to allow for the assumption that it may include – in the future – not only the personal data of persons directly interacting with EUSPA, ESA and the service providers related to the Copernicus programme, but also satellite, EO, geolocation (GALILEO) and telecommunication data which, as a result of appropriate processing or by reason of their specific characteristics, are such as to take on the typical characteristics of personal data as set out in Art. 4 of Regulation (EU) 2016/679 (also known as GDPR).

The European Union has therefore shown that it is well aware that any kind of satellite data, is capable of damaging people's privacy by adopting an approach to monitor and limit the dissemination of EO data. However, as interesting as the EU framework is, it should not be forgotten that it applies to European space policies, so it does not apply to private companies.

4. A combination of licensing procedures with privacy assessment?

Given what has been said in the preceding paragraphs, it is clear that there is a need to innovate the regulatory framework and the approach in general.

Therefore, the following questions will be addressed below: when can EO data become personal data? When is the highest level of privacy risk reached?

[30] Regulation (EU) No 377/2014 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0377.
[31] Regulation (EU) 2021/696 - https://eur-lex.europa.eu/eli/reg/2021/696/oj.

How could privacy verification be reconciled with preparatory activities for obtaining authorisations to operate in space?

4.1. When can EO data become personal data?

Regarding the first two questions, in order to verify whether EO data are capable of becoming personal data, it will be necessary to analyse the following elements on a case-by-case basis: (1) the type of sensor; (2) the spatial resolution of the sensor; (3) the revisiting time of the satellite or satellite constellation; 4) the possibility of combining them with other data, including data from other satellite sensors and other types of data (e.g. cadastral data); and (5) the level of dissemination and the procedures adopted to allow access to EO data.

Indeed, while it is true that there is a plurality of sensors currently used for Earth observation, it is equally true that only a few of these are capable of producing images perceived as such by us. If one looks at the images produced by IR sensors[32], it is difficult to perceive anything other than differences in temperature or in the absorption of infrared radiation. It follows that only certain types of sensors, such as optical sensors (which immediately produce true images) or SAR sensors (whose data lead to the creation of 'images'), are currently capable of producing data that can be used "immediately". Indeed, it is with these sensors that it is possible to distinguish buildings, moving vehicles and, in the near future perhaps, people.

The second element, the spatial resolution of a sensor, is in turn influenced by three different factors: 1) the technological development - already mentioned - on the ability to acquire increasingly better-defined images; 2) the positioning of an EO satellite at a lower orbit than usual (in which case it is the greater proximity to the subject to be imaged that allows for better-defined images); 3) the possibility of combining several images of equal resolution of the same area into a single image of better quality. On point 1), I will not add anything, but as far as factor 2) is concerned, it is necessary to point out that the recent licence (Tier 3) assigned to Albedo envisages precisely the use of EO satellites placed in VLEO orbit[33], i.e. at an altitude between 250 and 450 km, and this is enough to make one imagine how it is possible to obtain even better images. As for the possibility of fusing several images together to improve their quality, this is already a reality in consumer products (think of Olympus cameras, now OM System, equipped with a Hi Res Shot mode based on sensor displacement), so it was only a matter of time before the same concept was applied to much 'heavier' data, such as that produced by satellites[34].

[32] Earthdata-NASA, "Seeing Earth in a New Light", https://www.earthdata.nasa.gov/learn/articles/earth-ir-sensing.
[33] T. Hitchens, "Albedo catches Space Force eyes with ultra-high fidelity imagery from very low satellites", www.breakingdefense.com, April 2023.
[34] EUSI, "15cm HD imagery", https://www.euspaceimaging.com/15-cm-hd/. You can get the data sheet about Maxar imageri at https://www.euspaceimaging.com/15-cm-hd-imagery-by-maxar/. See also F. D. Javan, F. Samadzadegan, S. Mehravar, A. Toosi, R. Khatami, A. Stein, "A review of image fusion techniques for pan-sharpening of high-resolution satellite imagery", in ISPRS Journal of Photogrammetry and Remote Sensing, Vol. 171, 2021, 101-117.

The third element, then, is as important as any of the others. This is because, in order to have the most accurate data possible, it is (usually) not sufficient to have very high-resolution images of a given area. It is also necessary to have several images, staggered in time, of that same area in order to perceive the changes in it. It is in this sense that, for example, Maxar has planned to form a constellation of satellites capable of providing 15 daily revisits of a given area[35].

The fourth element, then, is particularly critical. We are currently in the era of big-data, i.e. in a historical period in which the fusion of data of different origins and types is now an established practice[36]. Therefore, making an assessment of the possibility of obtaining the complete picture of a data area through these practices is an essential element for a correct assessment of privacy risk.

The last element, i.e. the level and procedures of EO data dissemination, is only relevant if taken into account in conjunction with the previous elements. If there is a (potentially privacy-impairing) combination of the elements considered above, then the lesser or greater dissemination of EO data may be the decisive criterion for deciding whether or not there is a privacy risk in the concrete case under consideration. Below is an example to better render the concept (Fig. 1).

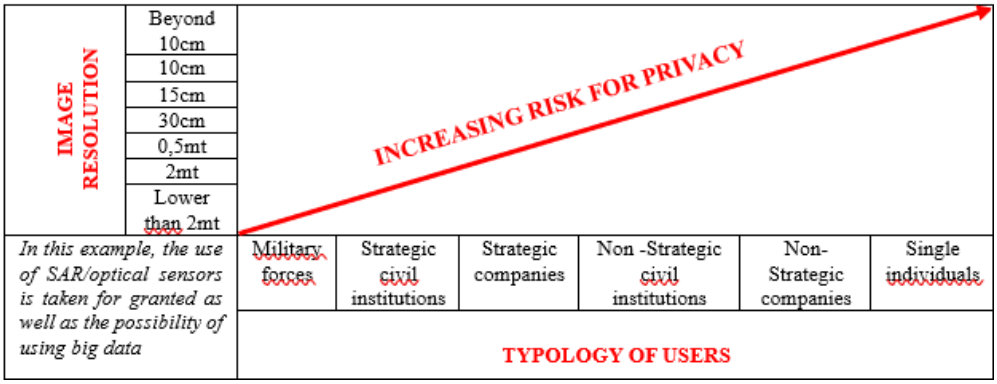


Fig. 1 - the relationship between dissemination and all other criteria

As can be seen, the risk arising from EO data, taking for granted the use of precise sensors and the possibility of exploiting big data, increases not only as the resolution of the images increases, but above all as the level of dissemination of possible users increases, dividing these into military forces, strategic civil institutions (such as civil defence, health, police forces, disaster relief), strategic companies (transport, energy, primary resources, telecommunications) and then non-strategic civil institutions and companies, and finally individuals. In fact, one could even divide that empty space within the table into four 'risk zones'. Well, any combination involving the dissemination to non-strategic civilian institutions, non-strategic companies

[35] Satellite Imaging Corporation, "WorldView Legion Satellite Constellation (30cm)", https://www.satimagingcorp.com/satellite-sensors/worldview-legion-satellite-constellation/.

[36] L. Zhao, X. Zhou and G. Kuang, "Building detection from urban SAR image using building characteristics and contextual information", in EURASIP Journal on Advances in Signal Processing, 2013 (56). J. D. Wegner, U. Soergel, R. Haensch and A. Thiele, "Fusion of high-resolution InSAR data and optical imagery for building detection using Conditional Random Fields", 8th European Conference on Synthetic Aperture Radar, Aachen, Germany, 2010, 1-4.

and individuals of EO data with a resolution of 15cm/pixel or better would fall within the maximum risk zone indicated by the red area (Fig. 2).

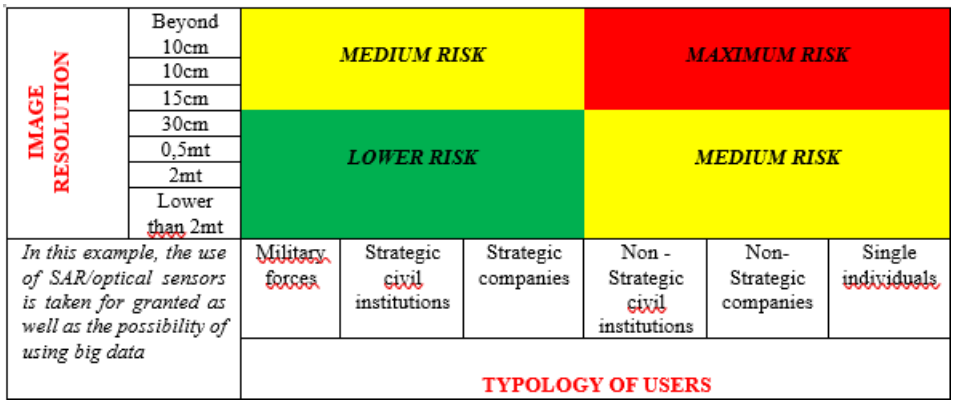


Fig. 2 - a variant of the previous table

It follows, therefore, that one of the most relevant criteria is the extent of EO data dissemination.

4.2. A first hypothesis: combining evaluation for ITU licences with privacy protection.

The evaluation outlined above is particularly complex, so it must be 'triggered' upon the occurrence of some precise precondition. This could be done by creating a link between the activities aimed at obtaining authorisations for space operations and those aimed at verifying data protection compliance.

For example, consider that operating a satellite requires a radio frequency link between the satellite itself and the control centre, which can be operated using a precise radio frequency.

To do this, however, it is necessary to obtain a special licence from the International Telecommunication Union (ITU), which deals with the allocation of radio frequencies. In fact, the radio spectrum is to be regarded as a finite good, not as an asset to which anyone who applies for it has unlimited access. Normally, relations with the ITU are taken care of by the same body that issues, at national level, the licences to operate a satellite (in the United States, in fact, it is NOAA that deals with this[37]).

So, let us assume that a company applies for licences (including ITU licences) to operate an EO satellite with particularly high resolutions. In such a case, the licensing body would have to immediately liaise with the privacy protection body. While the former would verify compliance with the national security and technical design requirements of the satellite, the latter would carry out a privacy compliance check with regard to the dissemination and processing of EO data.

At the same time, it should be borne in mind that the use of SAR sensors itself requires a precise licence due to the physical principle that characterises

[37] NOAA, "Radio Frequency Management", https://www.noaa.gov/information-technology/ocio-programs/radio-frequency-management. See also ITU Radio Regulations Articles, Edition of 2020.

the operation of a 'radar', so much so that the ITU classifies it as 'active sensing', in contrast to the 'passive sensing' implemented with normal optical sensors. In fact, on p. 137 of the ITU-RRs (Edition of 2020) there is a table with the allocations of frequencies between 8,500 and 10,000 MHz, i.e. that part of the radio spectrum known as the 'X Band', which is particularly prized for the resolution of the images that are generated. Well, the fact that a company applies for an X-Band licence could itself be a prerequisite for initiating a privacy check on single companies. Similarly, should the opportunity arise to use other different radio frequencies (although physical limits, such as those due to atmospheric absorption, must be considered), should they provide even sharper images than those obtainable in the X-band, then a joint check by the national security (and space) authority and the privacy authority would again be 'triggered'.

5. Conclusions.

It is well known that EO data are essential in the current context[38], so much so that an open access policy is being pursued[39]. Yet, the democratisation of space and data has shown how EO data can become (in the future) personal data, although this has only recently emerged in academic research[40]. It is therefore necessary to adopt 'shutter control' type systems[41], but adapted from the military to the civil sphere, so as to limit the dissemination of certain types of EO data only within specific institutional or corporate environments, following a casuistic analysis as outlined above. Such limitations in dissemination could also be added to the use of EO data processing systems that precede dissemination and are in line with privacy protection[42].

[38] M. Obersteiner, J. Balkovič, H. Böttcher et al., "The Value of Global Earth Observations", in Satellite Earth Observations and Their Impact on Society and Policy (Masami Onoda • Oran R. Young, 2018), pp. 137-141.
[39] J. Aschbacher, "ESA's Earth Observation Strategy and Copernicus" in Satellite Earth Observations and Their Impact on Society and Policy (Masami Onoda and Oran R. Young, Editors), 2018, 81-85.
[40] C. Santos and L. Rapp, "Satellite Imagery, Very High-Resolution and Processing-Intensive Image Analysis: Potential Risks Under the GDPR", in Air and Space Law. 2019/44, pp. 275-295. ESPI, "Current Legal Issues for Satellite Earth Observation: Treaty Verification and Law Enforcement Through Satellite Observation, Privacy Conflicts from High Resolution Imaging", Report 25, August 2010.
[41] D.F. Dumaris Sitanggang, "International Law Analysis of The Restrictions Imposed on Remote Sensing Satellite Through Shutter Control", MIMBAR HUKUM Vol. 30, no. 2, (Halaman, June 2018), pp. 389-406.
[42] M. Alkhelaiwi, W. Boulila, J. Ahmad, A. Koubaa, M. Driss, "An Efficient Approach Based on Privacy-Preserving Deep Learning for Satellite Image Classification", Remote Sens. vol. 13, no. 11, 2221, Jun. 2021.