Space-Based Services Supporting Refugees

Legal Aspects

*Mahulena Hofmann, Gerome Aloisio and Loredana Rinaldis**

1. Introduction

Article III of the Outer Space Treaty[1] (OST) states that States Parties to the Treaty shall carry on activities in the use of outer space in the interest of maintaining international security and promoting international cooperation and understanding. During the drafting of the OST, this principle had a specific, East-West connotation. Today, in a changed geopolitical situation, the core message of this principle remains valid; however, the notion of "security" has acquired other connotations. Both international terrorism and the recent refugee crisis in Europe have brought about numerous new perils, one of the most serious one being the danger to the lives of those who use all their efforts to reach Europe and to settle in a safer part of the world than their own.

In the last three years, Europe has experienced the greatest mass movement of people since the Second World War. More than one million refugees and migrants arrived in the European Union with the large majority of them fleeing from war and terror in Syria and other troubled countries. The EU has agreed on different measures to deal with the crisis that range from attempts to resolve its root-causes to the supporting people in need of humanitarian

* Mahulena Hofmann, University of Luxembourg, SES Chair in Space, SatCom and Media Law. Gerome Aloisio, University of Luxembourg, Master in Space, Communication & Media Law. Loredana Rinaldis, University of Luxembourg, Master in Space, Communication & Media Law. Mahulena Hofmann, University of Luxembourg, SES Chair in Space, SatCom and Media Law. Gerome Aloisio, University of Luxembourg, Master in Space, Communication & Media Law. Loredana Rinaldis, University of Luxembourg, Master in Space, Communication & Media Law.

1 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, UNTS, vol. 610, No. 8843.

assistance both inside and outside the EU. Steps are being taken to relocate asylum seekers that are already in the EU, to resettle people in need coming from neighbouring countries, and to return those who do not qualify for asylum. This package of steps is complemented with improving the security at the frontiers of the Union with a specific border and coast guard, tackling people smuggling, and showing safe ways for people to legally enter the EU.[2]

It is no secret that almost all of these activities use data and information gained with the help of space-based technologies. To be able to assist the refugees through the national and European institutions, the European Union set up several frameworks that use Earth observation from outer space. This technology, combined with various categories of terrestrial data, assists in locating those in need. Additionally, the migrants rely on satellite-based services, such as navigation signals, for approaching Europe. Location based services (LBS), especially on smartphones, have become an important instrument allowing them to find the right trajectory. Some of the refugees have even reported that they would be "lost without Google Maps"[3] as throughout their journey they have used this application based on Global Navigation Satellite Systems (GNSS) signal using the services of GNSS satellites to cross both land and sea.

As both categories of services – Earth observation and geolocation – use signals from satellites orbiting the Earth, several questions arise that are the central interest of this contribution. First, is the use of space-based services a "space activity" in the sense of UN space law, and what are the consequences? Second, how is the use of space-based data for the support of refugees by the European authorities regulated?

2. Is the Use of Space Originated Observation and Communication Services "Space Activity" in the Sense of the UN Space Law?

There is no legal definition of space activities, more precisely of "activities in the exploration and use of outer space" in the present UN legal regime governing outer space. Without any spatial delimitation of the scope of international space law, this notion is open to extensive interpretation[4] and

2 Https://publications.europa.eu/en/publication-detail/-/publication/1aa55791-3875-4612-9b40-a73a593065a3.

3 B. Sebti, 4 smartphone tools Syrian refugees use to arrive in Europe safely, The World Bank, 17 February 2016, http://blogs.worlsbank.org/voicesa/4-smartphone-tools-Syrian.refugees.use-to-arrive.in-Europe-safely.

4 To compare, Article 1.64 of the ITU Radio Regulations stipulates that « space station" is a station located on an object which is intended to go beyond, or has been beyond, the major portion of the Earth's atmosphere. Similarly, "spacecraft" is defined as a man-made vehicle which is intended to go beyond the major portion of the Earth's atmosphere. (Article 1.178).

its possible extension to activities executed not only in outer space but, also, on the Earth. As stated in the *Cologne Commentary on Space Law*,[5] in the 1960s there was general consensus that space activities are not confined to those carried out "in" outer space, and this term can also include activities "connected" to the launching, the operation, or the return of space objects.
However, the link between a space object and a specific activity cannot be too long or too loose to evoke the application of UN space law in endless circumstances.[6] The elaboration of the recommendatory principles covering direct television broadcasting using satellites,[7] and remote sensing of the Earth from outer space[8] in the framework of UNCOPUS and its Legal Subcommittee as "legal problems which may arise from the exploration and use of outer space"[9] seem to be been rather an exception from their legislative efforts focused primarily on space activities *stricto sensu*.
The scope of the above-mentioned 1986 *UN Remote Sensing Principles*[10] shows the closest technological resemblance to the Earth observation used for the geolocation of migrants and the protection of external EU borders. However, this recommendatory regime is limited to handling space-based data on "improving natural resources management, land use and the protection of environment, rather the observation of movements of persons. "Remote sensing activities" are defined as "the operation of remote sensing space systems, primary data collection and storage stations, and activities in processing, interpreting and disseminating pro processed data" (Principle I (e)), which clearly includes activities on the Earth and not only in outer space. *Per definitionem*, the collection of data and information using space-based technology is combined with "inputs of data and knowledge from other sources" (Principle I (d)). Interestingly, the Principles require that remote sensing activities be conducted in accordance with international law, including also the Outer Space Treaty (Principle III). In the body of the Principles, however, only Principle XIV declares that States operating remote sensing "satellites" shall bear international responsibility for their activities in compliance with Article VI OST. Other "remote sensing activities" are

5 CoCoSl, Volume 1, 2009, p. 66.
6 Compare e.g. with the case of control and guidance of UAVs, F. von der Dunk, Unmanned Aerial Vehicles, Their Use of Satellite Services and (Space) Law, in: M. Hofmann/ P.J.Blount (eds.), Innovation in Outer Space: International and African Legal Perspectives, 2018.
7 Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting, adopted by the General Assembly in its resolution 37/92 of 10 December 1982.
8 Principles Relating to Remote Sensing of the Earth from Outer Space, Adopted by the General Assembly in its resolution 41/65 0f 3 December 1986.
9 Preamble of the UN Resolution 1721 A and B (XVI) of 20 December 1961.
10 UN GA Res. 41/65 of December 1986.

subsumed into the generally applicable "norms of international law on State responsibility."

What is the consequence of this analogy? The differentiation between the responsibility regime for operation remote sensing "satellites" and the applicability of general norms of international responsibility to the rest of remote sensing "activities" leads to the conclusion that in the case of other space based services like Earth observation or navigation UN space law is only relevant to the part connected with the launching and operation of "space objects." The UN space treaties will not be applicable to collecting data and information using space based stations. The responsible entity for the service and bearer of eventual liability for damage caused from the consequences of the use of this category of services would not be the "appropriate State Party" in the sense of Article VI OST or "the launching State" according to Article VII OST, but the provider of the service.[11] Only the material damage caused by the satellite(s), its component parts and the launch vehicle(s) would be attributable to one the "launching States" of the satellite (Article VIII OST) and guided eventually by the regime of the 1972 UN Liability Convention.[12]

3. How Has the European Union Regulated the Collection and Use of Space-Based Data Supporting Refugees?

3.1 Programme Copernicus

One of the specific objectives of the EU programme *Copernicus* as per Article 4.2.(a) is to provide access to comprehensive and accurate space-based information supporting the protection of the environment and of the population, e.g. for border surveillance. It was established in 2010 through the Union's Regulation No 911/2010 that established the basis and initial operations of the Earth observation programme *Global Monitoring for Environment and Security* (GMES).[13] This regulation was replaced by the 2014 *Copernicus Regulation,*[14] which was accompanied by a 2013 *Delegated Regulation (EU) No 1159/2013* on the registration and licensing conditions

11 See A. Loukakis, Non-Contractual Liabilities from Civilian Versions of the GNSS, 2017, 173 ff.

12 Convention on International Liability for Damage Caused by Space Objects, UNTS, vol. 961, No. 13810.

13 Regulation (EU) No 911/2010 of the European Parliament and of the Council of 22 September 2010 on the European Earth monitoring programme (GMES) and its initial operations (2011 to 2013), (O) L 276, 20.10.2010.

14 Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010, (O) L 122, 24.4.2014.

for Copernicus users.[15] In October 2014, the operations of the Copernicus constellation – the Sentinels – started with the launch of Sentinel-1A,[16] one of its planned six satellite families.

According to article 28.1 of the Copernicus Regulation, the European Union holds the ownership of the Programme along with its tangible (ground and space segment as well as in situ components) and intangible (services and products) assets. The European Commission serves as its coordinator and the owner of the Sentinel satellites, with the plan later to create a constellation of more than twelve Sentinels supported by the European Earth observation satellites of "the contribution missions."[17] Furthermore, the Commission is the institution designated to manage the Programme, to ensure its optimal use of assets, to manage intellectual property rights, and the development of the services along with its sustainability and take-off of EO markets. It is also the Commission that is the entitled entity to elaborate contracts on behalf of the Union such as tenders of services and information distribution platforms. Pursuant to the Agreement between the European Union, represented by the European Commission, and the European Space Agency on the Implementation of the Copernicus Programme, including the Transfer of Ownership of Sentinels (Copernicus Agreement) that entered into force on 28 October 2014, the ownership of the satellites belonging to the Copernicus programme is transferred to the European Union at the moment of lift-off of the satellite's launch vehicle.[18] The European Space Agency has been delegated the responsibility of manufacturing the space segment and operation of the satellites – together with *Eumetsat*.[19] This engagement has been agreed by the Commission and ESA to be held until 2021, which is the period that the budget of the Union has been secured at the time of writing.[20]

Several European agencies are using and distributing data of the Copernicus programme, such as the European Entrusted Entity (EEE) and the European Agency for the Management of Operational Cooperation at the External

15 Regulation (EU) No 1159/2013 of the European Parliament and of the Council on the European Earth monitoring programme (GMES) by establishing registration and licensing conditions for GMES users and defining criteria for restricting access to GMES dedicated data and GMES service information, (O) L 309, 19.11.2013.

16 European Space Agency, First Copernicus Satellite Now Operational, www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Sentinel-1/First Copernicus_satellite_now_operational.

17 Contributing Missions, www.copernicus.eu/main/contributiong-missions.

18 See also I. Thoma, Transfer of Satellites in Orbit: the ESA Experience, in: M. Hofmann/ A. Loukakis (ed.), Ownership of Satellites, 2017, 107 ff.

19 European Commission, Copernicus – Europe's Eye on Earth, 2015, http://copernicus.eu/sites/default/files/documents/Brochure/Copernicus_Brochure_EN_WEB.pdf.

20 European Space Agency, Copernicus Operations Secured until 2021, www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Copernicus_operations_secures_until_2021.

Borders of the Member States of the European Union – *Frontex*,[21] which has been assigned the task to control and manage the EU's outer borders (Article 1 of the 2016 *Frontex* Regulation). The Commission entrusted this Agency with the Security Service of the Copernicus Programme dedicated to the Union's border surveillance . This service is one of the six services of the Programme established under a delegation agreement signed in 2015 between the Commission and Frontex.[22]

Frontex cooperates closely with EU Member States through Frontex's information-exchange system *Eurosur* (European Border Surveillance System).[23] This information exchange platform that enables real-time sharing of border related information[24] is based on the *Regulation Establishing the European Border Surveillance System* of 2013.[25] This multipurpose network for cooperation between the EU Member States and Frontex in intended to prevent cross-border crime and irregular migration and to contribute to the protection of migrant lives.[26] The situational awareness is supposed to be achieved with the help of the information exchange between Frontex, and national authorities responsible for border surveillance.

On the basis of the Service Legal Agreement, concluded in May 2015 between Frontex and *European Satellite Centre* (SatCen), many Frontex services are delivered in cooperation with the SatCen, a decentralized EU agency.[27] SatCen supports Frontex "in its effort to monitor coastal and external border activity related to the migration crisis" by providing products resulting from the exploitation of, *inter alia*. space assets and satellite imagery.

The maritime surveillance service of Copernicus is managed by the *European Maritime Safety Agency* (EMSA). On the basis of the *Frontex* – EMSA Agreement,[28] EMSA supports Member States to perform border surveillance,

21 Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC, (O) L 251, 16.9.2016.

22 Copernicus Security Service, http://copernicus.eu/main/security.

23 Http://frontex.europa.eu/intelligence/eurosur.

24 J. Rijpma, R. Vermeulen, Eurosur: Saving Lives or Building Borders? European Security, 2015, p. 454.

25 Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance system (Eurosur), (O) L 295, 6.11.2013.

26 European Commission, Eurosur, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/eurosur-en.

27 European Union Satellite Center, Annual Report 2016, p. 15, https://www.satcen.europa.eu/key_documents.

28 Frontex, EMSA and EFCA extend cooperation, http://frontex.europa.eu/news/frontex-emsa-and-efca-extend-cooperation-eIXD0P.

in the interception of vessels suspected of engaging in criminal activities, in the prevention of cross border crime, and in search and rescue at sea.

3.2 Surveillance and Processing Personal Data

During its activities, the border surveillance service of European Union gathers large amounts of data, including data received from sensors installed on-board of satellites belonging to the Copernicus programme. This data, processed and combined with information from other sources, is a powerful tool for the support and rescue refugees and migrants. At the same time, this data might constitute a risk to the privacy of persons in the surveyed area as they can provide information about persons and make them "identifiable" in the sense of Article 2 (a) of the EU 1995 *Data Protection Directive* No 95/46.[29]

Surprisingly, the 2014 *Copernicus Regulation*[30] does not establish any specific rules concerning the regime of dealing with personal data, despite of the fact that it stipulates that the programme should be implemented consistently with the instruments in the field of protection of personal data (recital 9). This is done primarily by reference to delegated acts concerning, *inter alia,* the criteria and procedures for the restriction of acquisition or dissemination of Copernicus data and information due to conflicting rights (Article 24 (1 c)). Recital 12 of this delegate act, the 2013 *Commission Delegated Regulation,*[31] requires that the Commission applies restrictions to the full free and open Copernicus data policy if the access to these data would conflict with the fundamental rights enshrined in the Charter of Fundamental Rights of the EU. Furthermore, according to its Article 11, the Commission shall take measures to avoid or restrict the access to Copernicus data that could affect the right to data protection "in a disproportionate manner." These unspecified measures are further mentioned in "GMES data and information policy" of the 2010 GMES Regulation (Article 9)[32] and lead only to the non-surprising conclusion that this is the Commission who is responsible for implementing the data protection in relation to the data obtained from the Copernicus programme.

The 2016 *Frontex Regulation*[33] provides in its recital 47 that Frontex and its agents should fulfil their tasks in respect for fundamental rights, including the

29 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and of the free movement of such data, OJ L 281, 23/11/1995: "An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specified to his physical, mental, economic, cultural or social identity".

30 *Supra* note 14.

31 *Supra* note 15.

32 *Supra* note 13.

33 Regulation (EU) 2016/1624.

right to privacy and data protection as stipulated by the Charter and the ECHR, and it should develop and implement a strategy to monitor and ensure the protection of fundamental rights. Recital 57 foresees that "any processing of personal data by the Agency within the framework of this Regulation" should be conducted in accordance with *Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institution*s.[34] According to Recital 58, where the processing of data is necessary for the purpose of ensuring internal security within the Union, especially in the context relating to the monitoring of migratory flows and risk analysis or on the processing of personal data collected during joint operations or by migration management support teams, *Council Framework Decision* 2008/977/JHA *on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters* applies,[35] thus any processing of personal data should respect the principles of necessity and proportionality.

Article 45 ff. of the *Frontex* Regulation deals specifically with data protection. The management board of the European Border and Coast Agency shall establish measures for the application of the Regulation (EG) No 45/2001,[36] and the transfer of personal data to authorities of third countries is prohibited. Article 46 enumerates the purposes for which personal data can be processed by the Agency, in which the term "processing" includes a broad category of operations, including the collection, storage and dissemination of data.[37] The regulation encompasses personal data collected during joint operations, pilot projects, and other support activities in the framework of the migration management support teams or during identifying and tracking vessels. Any processing shall respect the principle of proportionality and be strictly limited to personal data necessary for the enumerated purposes. According to Article 47, it is permissible to process personal data regarding persons suspected of migrant smuggling or persons who cross external EU borders without authorization, including license plate numbers, vehicle identification numbers, telephone numbers, or ship identification numbers that are linked to such persons and are necessary for investigating and analysing routes and methods used for illegal immigration and cross-border crime. These data shall be deleted as soon as they have been transmitted to EASO, Europol, or Eurojust or to

34 Regulation (EC) No 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, (OJ L 8), 12.1.2001.

35 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, (OJ L 350), 30.12.2008.

36 *Supra* note 34.

37 See Article 2 of the Regulation (EC) No 45/2001.

competent authorities of the Member States, and the storage period shall not exceed ninety days after the date of their collection. Only in "the result of risk analyses" shall data be anonymised.

Article 72 of the *Frontex* Regulation introduces a complaint mechanism applicable in cases of the violation of fundamental rights resulting from the activities of the Agency, including the right to data protection. The fundamental rights officer appointed by the management board shall be responsible for handling the complaints and forward them to the executive director of the Agency who shall ensure appropriate follow up. If a complaint is related to data protection issues, the data protection officer of the Agency shall be involved. This complaint procedure shall be announced by the Agency to all, including vulnerable persons (Article 72, para. 10). Without going into details of the procedure for processing personal data of those in the focus of Frontex, the last rule mentioned in the Regulations reveals the weak point of the system in that most of the persons whose personal data are collected from outer space will not be aware about the existence of this data. Consequently, the whole system can hardly be realistically applicable to them.

The 2013 *Eurosur* Regulation[38] provides for a legal framework of the surveillance of external land and sea borders of the EU and includes the monitoring, detection, identification, tracking, prevention and interception of unauthorized border crossings for the purpose of detecting, preventing, and combating illegal immigration and cross-border crime. One aspect of its scope being "contributing to ensuring the protection and saving of the lives of migrants" (Article 2). Also the Eurosur network uses Earth observation imagery (Article 9 para. 7 d) resp. satellite imagery (Article 12 para. 2 b). During monitoring activities, personal data might be collected; therefore, recital 13 of the Regulation underlines that any exchange of personal data in the European situation picture and the common pre-frontier intelligence picture should constitute an exception of the data protection policy. It also foresees that in cases where specific regulations do not provide a full data protection regime, the general data protection instruments, such as the Directive 95/46/EC, the Regulation (EC) No 45/2001,[39] and the Council Framework Decision 2008/977/JHA are applicable.[40]

Article 13 of the *Eurosur* Regulation is devoted specifically to processing of personal data. According to its para. 2, the only personal data which may be processed without restriction in the European situational picture and the common pre-frontier picture are "ships identification numbers." These shall

38 *Supra* note 25.

39 *Supra* note 34.

40 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008.

be deleted within seven days resp. two months of receipt by *Frontex*. Other personal data shall be processed in accordance with the general data protection instruments. Article 20 regulates the regime of the exchange of personal data in the cooperation with third countries. Such exchanges must take place on the basis of bilateral or multilateral agreements that comply with the EU fundamental rights, and any exchange of data within the *Eurosur* framework shall be "strictly limited to what is absolutely necessary" for the purpose of the Regulation. In particular, any exchange of information which provides a third country with information that could be used to identify persons or groups of persons whose request for international protection (asylum) is under examination, shall be prohibited (para 5).

The details of the regime provided by the Eurosur Regulation have been made available through the 2015 *Practical Handbook*,[41] which has been adopted by the Commission in 2015 in the form of a recommendation (Article 21 of the Eurosur Regulation). The addressees of the Handbook are EU Member States and, specifically, their authorities responsible for surveillance of the external land and sea borders, as well as the Agency (Frontex) and other EU bodies involved in Eurosur. The Handbook does not create any legally binding obligations and cannot be – in contrast to the Eurosur Regulation – invoked before national courts or tribunals (p. 5 of the Handbook). Its chapter 2.4, "Protection of fundamental rights and measures contributing to saving migrants' lives," reminds of the fact that, when collecting information during border surveillance activities, the right to private life and the protection of personal data of any person must be respected. According to the Handbook (part 3.2.9), each Member State is responsible for the security of personal data collected in the course of its activities and for compliance with national data protection rules and activities. Member States also have to ensure that, upon expiry of the data retention period set under national law, personal data are deleted or anonymised according to national law. Also in cases when Frontex notices personal data other than ship identification numbers, it must notify the owner (originator) of the data (e.g. the National Coordination Centres) and request the removal of that data from the system. During its activities, Frontex cooperates with the European Data Protection Supervisor.

3.2 Use of Geolocation

The next space-based service used in relation to refugees and migrants is geolocation relying on Global Navigation Satellite Systems (GNSS). At present, there are two operative GNSS programs, the US Global Positioning

41 Commission recommendation of 15.12.2015 adopting the Practical handbook for implementing and managing the European Border Surveillance System (EUROSUR Handbook), C (2015) 9206 final.

System (GPS) and the Russian Global Orbiting Navigation Satellite System (GLONASS),[42] with several others preparing their entry to the GNSS market.[43] The European Navigation Service Galileo belongs to this second category; its deployment phase is planned to be completed by 31 December 2020.[44]

Location-based services (LBS) using GNSS, especially on smartphones, have become an important instrument allowing the migrants to find the right trajectory to their desired destination, and the supporting authorities to locate those in need. The less known aspect of the use of LBS is the fact that to get directions, the users of these services must share their current whereabouts with a service provider.[45] Consequently, LBS providers could monitor their users without them being aware that they are being tracked.[46] The providers can also enable the access of these data to third parties.[47]

The most prominent legal issues connected with the use of these applications are again privacy and data protection, together with the liability for erroneous positioning.[48] "Location privacy" is usually described as a specific type of information privacy, which concerns the right of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others.[49] An additional problem for data protection consist in the fact that location data is difficult to anonymise[50] and entities with access to accurate location data are able to make inferences about many characteristics of their users.[51]

---

42 S. Spassova, A. Loukakis, The Legal Implications of Erroneous GNSS Signal, Resulting from Harmful Interference, in: Proceedings of the 58th Colloquium on the Law of Outer Space, 2015, p. 79.

43 Together with the EU programme Galileo, there are also BeiDou and Compass of China and QZDD of Japan.

44 To the status quo of Galileo programme see e.g. L. Mantl, Galileo Programme – New Legal Developments, in: M. Hofmann/ P.J. Blount (eds.), Innovation in Outer Space: International and African Legal Perspectives, 2018.

45 M. Herrmann, M. Hildebrandt, L. Tielemans, C. Diaz, Privacy in Location-based Services: An Interdisciplinary Approach, SCRIPTed, 2016, vol. 13, Issue 2, p. 146.

46 Art. 29 Working Party, Opinion 13/2011 on Geolocation services on small mobile devices, 881/11/EN WP 185, May 2011, p. 7.

47 R. H. Weber, The Digital Future – A Challenge for Privacy, Computer Law & Security Review, 2015, Vol. 31, p. 237.

48 F. von der Dunk, Legal Aspects of Navigation – The cases for privacy and liability: an introduction for non-lawyers, Coordinates Magazine, May 2015, http://mycoordinates.org/legal aspects-of-navigation.

49 According to M. Duckhaam, L. Kuklik, Location privacy and location-aware computing, in: R. Billen, D. Forrest, J. Drummond et all, Dynamic & mobile GIS: investigating change in space and time, CRS Press, 2006, 35-51.

50 P. Golle, K. Patridge, On the Anonymity of Home/Work Location Pairs, in: Y. Tobe (ed.), H. Tokuda, M. Beigl et al., Pervasive Computing, 2009, 390-397.

51 M. Gasson, E. Kosta, D. Royer, M. Meints et al., Normality Mining: Privacy Implications on Behavioural Profiles Drawn from GPS Enabled Phones, IEEE

In contrast to the processing of personal data collected by Earth observation satellites operated by the European Union, there are no specific European legal rules dealing with LBS. The fact that these services are mostly provided by private "information society services"[52] excludes them from the category of "electronic communication networks" in the sense of the Directive 2002/21[53] and, consequently, from the scope of the *E-Privacy Directive*,[54] which otherwise deals with the processing of personal data by the electronic communication sector. Therefore, "only" the general Directive No 95/46/EC[55] is applicable to the protection of users of the LBS at present. This situation might remain unchanged also after entering into force of a new *E-Privacy Regulation*[56] as this envisages that only those services that enable "communication" among the users will be covered by its scope.

This situation is reflected also in the framework of the European Galileo programme. The Regulation 1285/2013 on the implementation and exploitation of European navigation systems[57] requires that all personal data handled in the context of the tasks of this Regulation shall be processed in accordance with the applicable law on personal data protection as stipulated in the Directive No 95/46/EC.[58] Furthermore, it states that in its Article 31 that "the Commission shall ensure that personal data and privacy are protected during the activities of the system and that the appropriate safeguards are included therein."

This situation may change in the future with the new European *General Data Protection Regulation*,[59] which is envisaged to enter into force in 2018. The

---

Transactions on Systems, Man and Cybernetics, Part C: Applications and Review, 2011, Vol. 41, Issue 2, 251-261.

52 Art. 29 Working Party, Opinion 13/2011, p. 8.

53 Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communication networks and services, p. 33-50.

54 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector, OJ L 201, 31.7.2002, 37-47.

55 *Supra* note 29.

56 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and he protection of personal data in electronic communication and repealing Directive 2002/58/EC, 10.01.2017, COM (2017) 10 final, 2017/0003 (COD).

57 Regulation (EU) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European navigation systems.

58 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and of the free movement of such data, (O) L 281), 23.11.1995, 31-50.

59 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

scope of this Regulation shall extend to the services and to data subjects as far as their "behaviour" takes place within the Union (Article 2(2)). Article 4(1) includes "location data" expressly among the identifiers covered by the material scope of the Regulation. However, it is questionable whether the migrants using geolocation data will be capable of enjoying the strengthened significance of the consent of the data subject to the processing of his or her data (Article 7) or the remedies available to the data subject in cases of non-compliance of the data controller with the rules set down in the Regulation. Unfortunately, the Regulation does not qualify "location data" as "sensitive data" (Article 9) and leaves the protection incomplete. Only a minimal improvement can be expected from the upcoming procedural obligation of the operators of LBS to established independent data protection officers and to conduct data protection impact assessments in order to realise how risky the processing of geolocation data might be and which technological measures have to be implemented in order to comply with the Regulation.

4. Conclusion

The support of refugees, their geolocation in the situation of distress by the entities of European Union, and the use of geolocation data and services open questions both in public international and European law.

The question whether the use of space originated observation and communication services is "space activity" in the sense of UN space law and therefore subject of the UN space treaties must be answered in a differentiated manner. UN space law is of relevance only for the part connected with the launching and operation of "space objects." The UN space treaties will not be applicable to collecting data and information using space based stations. The responsible entity for the service and bearer of eventual liability for damage caused by the use of this category of services shall not be the "appropriate State Party" or "the launching State" according to Outer Space Treaty, but the provider of the service. Only the material damage caused by the satellite(s), its component parts, and the launch vehicle(s) shall be attributable to one the "launching States" of the satellite and guided by the regime of the 1972 UN Liability Convention.

The legal framework of the European Earth observation system recognises the relevance of the space based data as personal data, as long as these can serve as identifiers of subjects of observation, and extends the general principles of data protection to this category of information. Additionally, the *Frontex* Regulation introduces a complaint mechanism applicable in cases of violation of fundamental rights by the activities of the Agency including the right to data protection. The fundamental rights officer appointed by the management board is responsible for handling the complaints, and any processing shall respect the principle of proportionality and be strictly limited to personal data necessary for the enumerated purposes. The weak point of

the system is, however, the fact that most of the persons whose personal data are collected from outer space are not aware about this fact. Consequently, the whole regime can be hardly realistically applicable to them.

The users of the location-based services (LBS) using GNSS, especially on smartphones, must share their current whereabouts with a service provider. LBS providers could monitor their users without them being aware that they are being tracked and can enable the access to these data to third parties. In contrast to the processing of personal data collected by Earth observation satellites operated by the European Union, there are no specific European legal rules dealing with LBS at present, and there will be hardly a substantial improvement in the future. As the upcoming European General Data Protection Regulation does not qualify "location data" as "sensitive data," protection of this data remains incomplete. The upcoming procedural improvements will not deal directly with location data.

The result of this small analysis is sobering. Naturally, whenever collecting of data and information using space services is realised, whether by the European Union, its institutions, and EU Member States implementing the EU legal framework, the bearers of the Earth observation data and the users of the geolocation services do enjoy the rules of the *Charter of Fundamental Rights of the European Union* (Article 8) together with Article 16 of the Treaty on Functioning of the European Union protecting personal data. Naturally, they are several specialized legal instruments that adapt this regime to the collection of data with the help of satellite technology and some dealing with collecting information from geolocation services. By no means should refugees and migrants be exempted from this protection. In practice, however, if our information is correct and no important element of the chain is missing, the refugees and migrants can hardly profit from this legal framework as they most probably unaware of the protections.

Despite of the pragmatism of this approach and seeing rightly the priority of saving the lives of those who are the object of space-based cameras and services, some steps should be made in the future to bridge this enormous gap in real possibilities to enforce the rights attached to specific groups of persons. Furthermore, the question can be raised whether all this data is really "necessary," in the wording of human rights instruments. Problems will not arise from one or two pieces of information collected in the course of European observation or geolocation without the consent of their subjects but from the enormous quantities of data, which might be capable to violate the tiny frontiers of "necessity" and "proportionality."