

4-30-2021

THE ADMISSIBILITY OF EARTH OBSERVATION DATA IN LEGAL PROCEEDINGS: A CLOSER LOOK TOWARDS DATA IMAGING

Alif Nurfakhri Muhammad

Leiden University, Netherlands, alifnurfakhri@gmail.com

Follow this and additional works at: <https://scholarhub.ui.ac.id/ilrev>



Part of the [International Law Commons](#)

Recommended Citation

Muhammad, Alif Nurfakhri (2021) "THE ADMISSIBILITY OF EARTH OBSERVATION DATA IN LEGAL PROCEEDINGS: A CLOSER LOOK TOWARDS DATA IMAGING," *Indonesia Law Review*. Vol. 11 : No. 1 , Article 2.

DOI: 10.15742/ilrev.v11n1.662

Available at: <https://scholarhub.ui.ac.id/ilrev/vol11/iss1/2>

This Article is brought to you for free and open access by the Faculty of Law at UI Scholars Hub. It has been accepted for inclusion in Indonesia Law Review by an authorized editor of UI Scholars Hub.

THE ADMISSIBILITY OF EARTH OBSERVATION DATA IN LEGAL PROCEEDINGS: A CLOSER LOOK TOWARDS DATA IMAGING

Alif Nurfakhri Muhammad*

*Leiden University, Netherlands

Article Info

Received : 22 November 2020 | Received in revised form : 25 January 2021 | Accepted : 26 February 2021
Corresponding author's e mail : alifnurfakhri@gmail.com

Abstract

Space capabilities utilization, specifically Earth observation capabilities is not just limited to environmental protection and disaster mitigation, as was shown in the UN Principles on Remote Sensing. It can also be used to support law enforcement and legal proceedings in court. However, the technology of Earth observation is very complex and the process from primary earth observation data to analyzed information requires a degree of manipulation to create comprehensive data. Because of this, there is an issue of admissibility of Earth observation data in court. This article would like to answer the fundamental question on how can this data be admissible, beginning with the procedure to obtain it and to ensure the authenticity of the data, and finds that there are methods of Data Imaging and Digital Audit that may ensure its authenticity. It will also find that obtaining this data for evidence requires a process of special agreement that needs to be looked at more in the future.

Keywords: earth observation; evidence; legal proceedings; data imaging.

Abstrak

Penggunaan Ruang Angkasa, khususnya untuk observasi Bumi tidak saja terbatas untuk perlindungan lingkungan dan mitigasi bencana, sebagaimana diamanatkan dalam Prinsip-Prinsip PBB dalam Penginderaan Jarak Jauh. Ruang Angkasa juga dapat digunakan untuk menunjang penegakan hukum dan proses peradilan, baik di pengadilan nasional, maupun internasional. Namun, teknologi observasi Bumi merupakan teknologi yang rumit, mengingat proses pengolahan data yang didapatkan membutuhkan proses-proses manipulasi tertentu agar data tersebut dapat diterjemahkan dengan baik. Manipulasi ini menimbulkan suatu permasalahan dalam menggunakan data observasi Bumi sebagai alat bukti yang sah di pengadilan. Artikel ini dibuat untuk menjawab pertanyaan bagaimana suatu data elektronik menjadi alat bukti yang sah, dimulai dari prosedur memperoleh data tersebut, penjaminan keaslian, dengan mengajukan metode data imaging dan digital audit yang dapat memastikan keabsahan tersebut. Artikel ini juga menemukan permasalahan lain dalam memperoleh suatu data satelit secara khusus dan data elektronik secara umum untuk digunakan sebagai alat bukti yang membutuhkan suatu perjanjian internasional antar negara.

Kata Kunci: observasi bumi; alat bukti; proses peradilan; data imaging.

I. INTRODUCTION

A. Legal Aspects on the Usage of Earth Observation Data in Courts

The use of Earth Observation (EO) data as evidence in court and other legal proceedings, is no longer a new example of the benefits of Space to the development of procedural legal affairs. From its use in the environmental cases¹ to the proceedings of International Tribunals,² the degree of uses may vary, but its use has been instrumental in proving locations of certain kinds that cannot be confirmed from land or air. As mentioned, the use of EO data is not just limited to courts within national jurisdiction, but also in international tribunals. The use of EO data in court, however, was not originally intended to be when it was first conceptualized and applied in practice, which was mainly for military purposes and in its development,³ for resource management and disaster mitigation.⁴ It is also interesting to look at not just the benefits of it, but also, on how it can be legally used in court proceedings, in which the main purpose is to produce reliable, scientific evidence, which depicts places that are inaccessible with analog means.⁵

This paper would like to explore the procedural aspects of the use of EO data in court. It will start with the legal basis, which is mainly deduced from the Outer Space Treaty and the UN Principles of Remote Sensing. In this Part, this paper would also try to identify certain legal issues, mainly related to the admissibility, but also on the access to this data by the Sensing States and the Sensed States. Next, this paper will move to propose the idea of Data Imaging and Digital Signature to ensure the admissibility of EO data as evidence in court proceedings. It will also give some examples from various jurisdictions in Rules of Evidence pertaining to electronic evidence, which will be divided into regions. Finally, this paper will be concluded with some remarks on the suggestion for its future legal use.

B. Outer Space Treaty and UN Principles on Remote Sensing

1. Important Stepping Stone: Article I of the Outer Space Treaty

Like many other activities in Outer Space, Earth Observation is bound by the Outer Space Treaty.⁶ Article I of the OST stipulated that the use of Outer Space must be for the benefit and the interest of all countries irrespective of their degree of economic or scientific development.⁷ The benefits and interest of all States in this article means that these benefits shall be enjoyed not just by developed States with space capabilities, but also by developing States.⁸ These benefits and interests are not just limited to military

¹ Kris Deghe, *et al.*, "The Use of Satellite Imagery in Environmental Crimes Prosecutions in the United States: A Developing Area", in *Evidence from Earth Observation Satellites: Emerging Legal Issues*, ed. Ray Purdy and Denis Leung (Leiden: Brill, 2013), 65.

² Maureen Williams, "Satellite Evidence in International Institutions", in *Evidence from Earth Observation Satellites: Emerging Legal Issues*, ed. Ray Purdy and Denis Leung (Leiden: Brill, 2013), 195.

³ Atsuyo Ito, *Legal Aspects of Satellite Remote Sensing* (Leiden: Brill, 2011), 9.

⁴ See Principles X and XI of UN Remote Sensing Principles.

⁵ E.D. Macauley, "The Role Satellites Should Play in the Protection and Promotion of Human Rights, Including the Use of Earth Observation Satellites in Evidential Matters," accessed April 13, 2020 https://www.mcgill.ca/iasl/files/iasl/wef-mcgill_space-macauley.pdf.

⁶ Ito, *Legal Aspects*, 23.

⁷ Article I Paragraph 1, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, UN Treaty Series 610 no. 8843.

⁸ Tanja Masson-Zwaan and Mahulena Hofmann, *Introduction to Space Law* (Aalphen Aan den Rijn: Kluwer, 2019), 17.

or commercial interests, but also to establish Rule of Law within the jurisdiction of States by providing an efficient way of law enforcement and supervision through Remote Sensing/Earth Observation.⁹ Although not specifically mentioned, it can be argued that the understanding of the utilization of EO Data as evidence in order to establish Rule of Law, is part of the “benefits and interests” of all States. To further understand to what extent these benefits and interests are guaranteed, we must also look to the UN Principles on Remote Sensing.

2. Limited mentions of benefits in the UN Principles on Remote Sensing

The Outer Space Treaty as the principal treaty governing the activities of States in Outer Space was created to be broad in nature to encompass various aspects of activities of States within the Outer Space. It does not provide specific guidelines on the use of EO and its obtained data.¹⁰ In its development, to counteract this absence, the UN General Assembly agreed to certain principles in the remote sensing activities, that is the UN Principles on Remote Sensing.¹¹ The principles set out certain agreeable fundamentals that States may follow in their conduct of remote sensing activities. When it comes to the use of EO Data as evidence, there are some of these principles that may be applied as the underlying basis for it to be accessible not just to the Sensing States, but also to the Sensed States. These relevant principles are:¹²

- Principle II ensures that remote sensing activities are to be carried out for the benefit and in the interest of all countries, irrespective of their degree of economic, scientific, and technological development, with the consideration to the needs of developing States.
- Principle IV ensures that remote sensing activities are to be conducted following the principles contained under Article I of the Outer Space Treaty, and ensure that such activities are to be conducted with respect for the principle of full and permanent sovereignty of all States over its wealth and natural resources following the international law.
- Principle V, ensuring the promotion of international cooperation for remote sensing activities and making available opportunities for participation from other States.
- Principle VI persuades States to come into agreement for remote sensing-related activities, including establishment and operation of data collecting, storage, processing, and interpreting with a clear legal framework.
- Principle XII, which is particularly important to this matter, is on the availability of the remote sensing data, which shall be made available and accessible by the Sensing States to the Sensed States, including any analyzed information coming from remote sensing data, on a non-discriminatory basis, and under reasonable cost terms.

Based on these principles alone, we can take some conclusion that although there is no exact stipulation that can be taken concerning the usage of EO data as evidence

⁹ Ningna Wang and Rujun Yang, “The Application of Chinese High-Spatial-Resolution Remote Sensing Satellite Image in Land Law Enforcement Information Extraction,” *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences* 42 (2018): 1751.

¹⁰ Arianna Vettorel, “Global Positioning System Evidence in Court Proceedings and Privacy: The Case of Italy,” *Air and Space Law* 42 (2017): 297.

¹¹ UN Res 41/65 of 3 December 1986.

¹² UN Res 41/65.

in court, there is at least some ground in ensuring that States, or in this case Sensing States have the right to launch and operate remote sensing capabilities, taking into account Article I of the Outer Space Treaty and Principle IV of the UN Principles on Remote Sensing to gather evidence that may be used in legal proceedings, and in relation to the rights of Sensed States, according to Principle XII, they shall have availability of the data, provided that it can come into an agreement with the Sensing States.¹³

C. Identifying the Legal Issues: Availability and Admissibility

After establishing that there are reasonable legal grounds under international space law instruments to use EO data evidence in court, this part of the paper will now try to establish other legal issues related to its use in court. The first one is the availability of EO data, which focuses more on the Rights of Sensed States to data obtained as part of their sovereignty. In general, EO data is publicly available via open access which means that the data is easily and freely accessed through a specific application or software,¹⁴ for example, satellite images that are accessible through Google Earth. However, to supplement this data, some data obtained through commercial EO operation may also be obtained, although with established cost terms. This can be done to guarantee the quality, accuracy, and authenticity of the data, which will affect the admissibility of the data.¹⁵ Sensed States who wish to submit EO data as evidence have to make sure that the obtained data is authentic, and obtained through a proper legal channel.

Several issues may be identified concerning the availability of the data. The first one is which EO data has to be made available for legal proceeding purposes. There are two kinds of EO data; primary data or raw data, which is the unprocessed data at full resolution obtained from satellite sensors, and processed data, which is the data analyzed through sets of variables, such as geophysical, or space-time criteria.¹⁶ An EO data that will be utilized as evidence admissible to court proceedings must be made available in both forms to preserve the clear chain of evidence. However, as will be shown under the last part of this paper, EO data admitted as evidence, is only submitted in its processed form, often not in digital form.

The second problem relating to the availability of EO data is closely related to the commercially-made EO data, and the access to both raw and processed data, that is how can both data be obtained through commercial means for evidence, while at the same time fulfilling the copyright protection owned by the commercial enterprises owning this data.¹⁷ Commercial EO Data is normally not a publicly available document, and the use of it as court evidence may make these privately-owned data public, once it is included in a case report. A proper safeguard or copyright protection must be created to ensure that the data acquired for evidence, is not used for any other purposes.

¹³ Ray Harris, "Science, Policy, and Evidence in EO," in *Evidence from Earth Observation*, ed. Purdy and Leung (Leiden: Brill, 2012), 46.

¹⁴ Ito, *Legal Aspects*, 202.

¹⁵ Ito, *Legal Aspects*, 233.

¹⁶ "Data Processing Levels," NASA, accessed on April 5, 2021, <https://earthdata.nasa.gov/collaborate/open-data-services-and-software/data-information-policy/data-levels>.

¹⁷ Catherine Doldirina, "Open Data and Earth Observations: The Case of Opening Up Access to and Use of Earth Observation Data Through the Global Earth Observation System of Systems," *Journal of Intellectual Property, Information Technology, and E-Commerce* 73 (2015): 75.

Second, and the most important part is the admissibility of EO data, from a technical standpoint that is also identifiable in the UN Principles, is that EO data will come through all sorts of transformation, from the Primary Data or Raw Data to Processed Data, and any analyzed information that materialized from this data.¹⁸ This creates a major issue of admissibility since the digital nature of this data makes it vulnerable and prone to manipulation.¹⁹ The issue of admissibility means that there has to be an assurance that EO data submitted as evidence in court is free from manipulation, authentic, and with desirable quality and accuracy. The way to achieve this admissibility will be further discussed in the following part of this paper.

II. THE AVAILABILITY OF EO DATA: HOW CAN EO DATA BE OBTAINED TO BE USED AS EVIDENCE

As mentioned in the previous part, for EO data to be used as evidence in court proceedings, there are different ways for it to be made available, depending on the status of the data. EO data that is considered a public document can be accessed through an agreement between States. *First*, a Remote Sensing Agreement, either bilateral or multilateral. This agreement can vary in form, from Agreement of Cooperation, in which the Sensed States have full access of the EO capabilities of the Sensing States; Collaborative Agreement, in which the Sensing States agree to collaborate with the Sensed States in developing EO technologies; or Data Exchange Agreement, which focuses more on the access of data and analyzed information.²⁰ The issue with this kind of agreement is that, in its development, these agreements are mostly an International Science and Technology Agreement (ISTA), which focuses more on the utilization of EO Data in accordance with the UN Principles.²¹

Another type of agreement that may be concluded is a Mutual Legal Assistance Agreement. MLA Agreement is primarily focused on criminal investigation and often contained stipulations concerning extradition.²² Although in practice MLA Agreement for exchange of evidence exists, it is hard to conclude one, since an investigation in a State may not be a priority in States where digital evidence exists.²³ Moreover, existing MLA Agreements are strictly for criminal investigation, and primarily to exchange primary evidence, that is directly related to a crime,²⁴ which is different from EO data, since it was first submitted as possible evidence, only to the extent that was used as supporting evidence. Another foreseeable issue that may hinder the availability of EO data as evidence through an MLA Agreement is the different institutions that are responsible for the object and the exchange. For example, in the US, civilian Remote Sensing or EO operations are mainly conducted by the National Oceanographic and Atmospheric Administration (NOAA), while the request of evidence is submitted through the Department of Justice (DoJ). A specific agreement that opens the

¹⁸ Masson-Zwaan, and Hofmann, *Introduction*, 174.

¹⁹ Clemens Arzt, "Use of Satellite Imagery in Legal Proceedings," *Air and Space Law* 24 (1999): 196.

²⁰ Caroline S. Wagner, *International Agreements on Cooperation in Remote Sensing and Earth Observation* (Washington D.C.: RAND, 1998), 10.

²¹ Conclusion deduced from analyzing the list of ISTA Agreement between USA and various States in Wagner, *International Agreements*, 27-93.

²² Els de Busser, "The Digital Unfitness of Mutual Legal Assistance," *Security and Human Rights* 28 (2017): 164.

²³ Joshua I. James and Pavel Gladyshev, "A Survey of Mutual Legal Assistance Involving Digital Evidence," *Digital Investigations* 18 (2016): 24.

²⁴ James and Gladyshev, "A Survey," 24.

possibility of access to EO data as digital evidence that is accessible for both civil and criminal procedures needs to be created and concluded.

One existing international convention may be relevant to obtain publicly-owned EO Data, that is the Evidence Convention.²⁵ Under the Convention, a court from a State party can request the competent authority of another State party to obtain evidence, that will be used in the requesting States court proceedings.²⁶ The requesting court can do so by sending a letter of request, which specifies the identity of the requesting authority, disputing parties, the nature of the proceedings that require evidence to be made available, and what evidence are requested to be made available by the requested States.²⁷ The Convention also specifies that special methods or procedures may be implemented in obtaining certain pieces of evidence unless the mentioned special procedures are incompatible with the internal law of the requested State.²⁸ Finally, should certain special methods or procedures require the involvement of experts or interpreters relating to the requested evidence, the requested State may require the requesting State to reimburse any costs arising from the use of these experts.²⁹

There are advantages or disadvantages when requesting evidence using the convention. The advantage is that a requested State cannot refuse to give evidence when a letter of request has been submitted, merely, it can inform the requesting State to readjust its request to be in conformity with its law, or refer the letter to relevant competent authorities.³⁰ The disadvantage in the application of this convention is that some States may enact a national law, with specific reference to data protection.³¹ The data protection law can be enacted to bar electronic evidence to be given, if the requested State finds that the requesting State has no or minimal legal protection to the data given, for example, to privacy protection, or proper copyright protection.³² This disadvantage is relevant when it comes to using EO data as evidence, since the requested EO data may contain personal information of the disputing parties that may be interpreted or used for purposes other than evidence in court proceedings.

Based on the discussion above, there are ways for the Sensed States, or the disputing parties in a Sensed State to be able to gain access or make available EO data to be submitted as evidence in a court proceeding. However, all of the agreement options only open the possibility of gaining publicly-owned EO data. Commercially-owned EO data by private entities can only be purchased, and only be able to be given in its processed form. To get the raw data needed from commercial EO data, a model purchase contract is the only way to get the entire data. Data protection and copyright law must also be established to protect this commercial EO data from publication outside of the court proceedings.

²⁵ *Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters*, UNTS Vol. 847 No. 12140.

²⁶ *The Hague Evidence Convention*, Article 1.

²⁷ *The Hague Evidence Convention*, Article 3, Paragraph 1.

²⁸ *The Hague Evidence Convention*, Article 9.

²⁹ *The Hague Evidence Convention*, Article 14.

³⁰ *The Hague Evidence Convention*, Article 5 and 6.

³¹ Brian Friederich, "Reinforcing the Hague Convention on Taking Evidence Abroad after Blocking Statutes, Data Privacy Directives, and Aerospace," *San Diego International Law Journal* 12, no. 1 (2010): 273.

³² Friedrich, "Reinforcing the Hague Convention," 273.

III. THE ADMISSIBILITY PROBLEM: HOW AUTHORITIES CAN USE EO DATA IN LEGAL PROCEEDINGS

A. The Process of Data Imaging with Digital Signature

Another issue at hand when it comes to utilizing EO data as evidence in legal proceedings is admissibility. To achieve this, there needs to be a rigorous process of “scrutiny” to ensure the authenticity, accuracy, and quality of EO data. One way to achieve this is the process of Data or Digital Imaging, and Digital Audit. Before discussing closer to this process, we must first understand the process of how Primary EO data is interpreted to become analyzed information.

Primary EO data or raw data collected from EO satellites are inherently manipulated by their interpreting instruments and sensors in a process called *image rectification and restoration*,³³ to produce more coherent data that is geometrically correct called “processed data”.³⁴ After this, processed data is further processed through enhancement, classification, and data merging to produce analyzed information.³⁵ This whole process is not without vulnerability. Potential errors during the interpretation of raw data into processed data always exist.³⁶ Therefore, a special calibration and specific digital signature must be assigned to each image data taken.³⁷

The existence of a Digital Signature is essential to the process of Data Imaging. Data Imaging is a process to create an exact copy of digital data, a bit-by-bit copy of the original data that, in the process, must also include some means to verify the authenticity of the copy and the reliability of the copying process.³⁸ During this process, a digital copy of EO data is created using special toolkits that preserve the bit formation and digital signature from the original storage, to achieve data reliability and authenticity.³⁹ This digital signature is generated and applied using a *Public Key Infrastructure*, that creates a digital “key”, which grants access only to the creator of the data, and the intended users.⁴⁰ A Digital Signature can also be in form of a certificate that is produced by a “Trusted Third Party” that issues digital certificates to data and access only to intended users.⁴¹

B. Digital Audit: Ensuring the Authenticity of Digital Signature

The next process, that must be considered, is the process of Digital Audit, to prove that this EO data has a clear, documented history on the whole steps of its process to be analyzed information. Concerning EO data, authenticity and accuracy are the two important matters to consider when conducting this digital audit.⁴²

- Authenticity, in which the auditor must prove that the EO data is authentic and

³³ James and Gladyshev, “A Survey,” 24.

³⁴ Harris, *Evidence in Earth Observation*, 58.

³⁵ Arzt, “Use of Satellite,” 196-97.

³⁶ Kenneth J. Markowitz, “Legal Challenges and Market Rewards to the Use and Acceptance of Remote Sensing and Digital Information as Evidence,” *Duke Environmental Law & Policy Forum* 12 (2002): 236.

³⁷ Markowitz, “Legal Challenges,” 236.

³⁸ Rodney Mckemmish, “When is Digital Evidence Forensically Sound?,” in *Advances in Digital Forensics IV*, ed. Indrajit Ray and Sujeet Sheno (New York: Springer, 2008): 5-6.

³⁹ Mckemmish, “When is Digital Evidence,” 6.

⁴⁰ Willibald Croi, *et al.*, “Introducing Digital Signatures and Time-Stamps in the EO data Processing Chain,” in *Evidence in Earth Observation*, ed. Purdy and Leung, 382-83.

⁴¹ Croi, “Introducing Digital,” 387.

⁴² Ito, *Legal Aspects*, 233-34.

has no unintentional or non-procedural manipulation or misinterpretation of the data. To achieve this, the history of the EO data must be documented in detail, from the moment it was captured by the satellite sensor until it becomes processed data and analyzed information, also including transfer processes between storage to users of data.

- Accuracy, in which the auditor has to make sure that the EO data used, is reflecting the actual phenomena on the observed surface of the Earth. This can be done through the process of calibrations, corrections, and ground truth measurements.

In the early days, the use of aerial photographic evidence, or images as evidence, courts in various jurisdictions acknowledged the need to authenticate images submitted by either producing a “witness” who directly produced or processed an image.⁴³ Another way is to produce an expert that can identify the accuracy and reliability of a picture.⁴⁴ However, digital images produced by EO satellites are different, as was shown from the complicated processes that they must go through to produce admissible information. Hence, there is the need for a specific audit or authentication process for EO data.

One way to see this is to look at the established practice in digital forensics. The process used by digital forensics involves three important stages. First, the recovery, where forensics experts are responsible for extracting the data, examining, and re-encrypting to make sure that it does not lose its digital signature.⁴⁵ Second, the interpretation, in which forensic experts analyze and interpret data, by synthesizing similar information through different sources and comparing the two data samples, to ensure as little difference as possible.⁴⁶ The final stage is the presentation, in which the analyzed data is presented, either to investigators or directly in court as testimony.⁴⁷ These audit procedures must be done by both the forensics who created the first copy, and by an independent third party who authenticate or re-audited the procedures.⁴⁸

IV. EXAMPLES FROM SEVERAL JURISDICTIONS

A. The EU Member States and the other European States

From the European Perspective, there have been movements towards treating digital evidence with the aforementioned level of security since 1999 with the Directive 1999/93/EC which contains stipulations on the legal effects of electronic signatures.⁴⁹ Article 5 of the directive suggested that member-States shall ensure that on every electronic data to be embedded electronic signatures created by a secure-signature device, that has the same value of a handwritten signature, in which this data should be admissible as evidence in legal proceedings.⁵⁰ It is safe to say, that the EU Member-States in principle, acknowledges the procedural aspect of admissibility of electronic evidence through this basis alone. In a recent development, the EU has published a guideline in 2019 for electronic evidence in civil and administrative

⁴³ Kristopher R. Hufstetler, “The Admissibility of Aerial Photographs - Evidentiary Foundations”, *St. Mary's Law Journal* 47 (2016): 860.

⁴⁴ Hufstetler, “The Admissibility,” 861.

⁴⁵ UK Parliamentary Office of Science and Technology, *Digital Forensics and Crime*, 520 Postnote (2016), 2.

⁴⁶ UKPST, *Digital Forensics*, 2.

⁴⁷ UKPST, *Digital Forensics*, see also UK Association of Chief Police Officers, *Good Practice*, 11-12.

⁴⁸ Mckemish, “When is Digital Evidence,” 7.

⁴⁹ Croi, “Introducing Digital,” 381.

⁵⁰ Croi, “Introducing Digital,” 381.

proceedings.⁵¹

The principles set by the 1999 directives were shown in the development of rules of evidence in the various EU Member States. For instance, in the Netherlands, any electronic data may be submitted as evidence, so long as it fulfills the requirements set by Article 3 Paragraph 15a of the Dutch Civil Code, which is that this data must have an electronic signature.⁵² The electronic signature mentioned must also be produced through a qualified certificate, in accordance with the Dutch *Telecommunicatiewet 1998*.⁵³

In terms of availability of electronic evidence, the EU Member States are parties to the Cybercrime Convention, which in its Article 25 Paragraph (1), obliges State Parties to assist other parties for investigations or proceedings which involve computer systems and data.⁵⁴ The convention leaves the interpretation of its broad stipulations on the aid to its State Parties, to open the possibility to obtain and utilize all kinds of electronic evidence available.⁵⁵ However, this convention is strictly on criminal matters, particularly those which have close relations to Cybercrime. The possible availability to use in civil or administrative proceedings lies strictly in the national law of Member States.

B. Asia Pacific Countries (With Special Notes to Indonesia)

Unlike in Europe, where there is a supranational organization that may publish directives or guidelines to set standards on electronic evidence regionally, Asia Pacific is more sporadic, but each national Rules of Evidence has followed the same aforementioned principles and processes. In Singapore, the Evidence Act, albeit an old one, recognizes through its development that any relevant evidence may be submitted, so long as it is properly obtained.⁵⁶ From electronic evidence standing, Singapore treats EO data as “documentary evidence” which is any matter expressed or described on any substance by means of letters, figures, or marks or by any other matter.⁵⁷ In this case, Singapore in the Criminal Procedure Code, also opens the possibility of EO data to be used, either as photographic evidence or as any other image types, so long as it follows the aforementioned procedures on authentication.⁵⁸

Indonesia, on the other hand, has plenty of legal safeguards concerning the use of electronic evidence. The core legal basis for using electronic data of any kind in Indonesia is Law No. 11 of 2008 on Electronic Information and Transaction,⁵⁹ with its amending Law No. 19 of 2016.⁶⁰ The law defines electronic information as,

⁵¹ European Council, *Guidelines for Electronic Evidence in Civil and Administrative Proceedings* (2019).

⁵² C.H. van Rhee, *Evidence in Civil Law – The Netherlands* (2012), 17.

⁵³ Van Rhee, *Evidence*, 17.

⁵⁴ J.P. Mifsud Bonnici, *et al.*, “The European Legal Framework on Electronic Evidence: Complex and in Need of Reform,” in *Handling and Exchanging Electronic Evidence Across Europe*, ed. M. A. Biasiotti, J. P. Mifsud Bonnici, J. Cannataci, and F. Turchi (Germany: Springer, 2018), 202.

⁵⁵ Bonnici, “The European Legal Framework,” 202.

⁵⁶ *Cheng Swee Tiang v PP*, MLJ 291 (1964), see also Gerardine Goh Escolar, *The Use of EO Data as Evidence in the Courts of Singapore*, in *Evidence from Earth Observation Satellites: Emerging Legal Issues* 93, ed. Ray Purdy and Denis Leung (2013): 96-97.

⁵⁷ Escolar, “The Use of EO Data,” 99.

⁵⁸ Section 378(3), *Singapore Criminal Procedure Code.*, Escolar, 101.

⁵⁹ Indonesia, *Law No. 11 of 2008 on Electronic Information and Transaction* (State Gazette 2008 No. 58).

⁶⁰ Indonesia, *Law No. 19 of 2016 amending the Law No. 11 of 2008 on Electronic Information and Transaction* (State Gazette 2016 No. 251).

“One or a collection of electronic data, including but not limited to writings, sounds, pictures, maps, designs, photograph, electronic data interchange, electronic mail, telegram, telex, telecopy of any kind, alphabets, numbers, markings, access codes, symbols, or any kind of perforation which has been processed and have a defined meaning, or understood by people deemed able to understand its defined meaning.”⁶¹

Based on this definition, Indonesian law seems to try to open the regulation for the use of all kinds of data as evidence. This is also strengthened by Article 5 of the Law, which stipulates that any electronic information or electronic documents, or its imprints, shall be admissible as evidence, which is defined as the extension of “evidence” stipulated under the Indonesian Code of Criminal Procedure.⁶² The Electronic Information and Transaction Law also stipulates that an “electronic system” of procedure must be taken for such information or document to be made admissible as evidence.⁶³ The Government Regulation No. 71 of 2019, narrows down the procedure into three components: the electronic system itself, which is a system of hardware and electronic procedure that is used to prepare, collect, process, analyze, store, show, publish, send, or share electronic information;⁶⁴ the electronic system organizer, which is an authorized individual, private entity or government institution who operates an electronic system for own use or the use of other entities;⁶⁵ and the electronic signature system, which consists of an electronic signature, electronic signatory, and an electronic signature software.⁶⁶

Although the procedural components have been set out under the Law and Regulation, the actual procedural steps are still unclear and sporadic. This is self-evident when looking at several of the cases that utilize electronic information, specifically earth observation data as evidence in court proceedings. In *Yayasan Riau Madani v PT. Chevron Pacific Indonesia*,⁶⁷ earth observation data was used as evidence to point out an area supposedly polluted when a waste disposal facility was built in an area designated as a recreational forest. In this case, the claimant submitted a printed version of an image produced by the LANDSAT-4 Satellite, but not authenticated digitally; merely authenticated by an expert who retrieved the image from the National Land Bureau. Moreover, in *Melanthon Manurung v PT. Ruas Utama Jaya*,⁶⁸ the printed version of satellite image used to pinpoint the location of disputed land, not an authentic copy, merely a photocopy of a photocopy, not authenticated by any expert whatsoever. One can argue that this happens because of the lack of regulatory requirements to admit such evidence in court since it was done before the 2019 Regulation.

However, when we look at the cases decided in 2019, we also see similar patterns of admitting the printed version or a photocopy of earth observation images as evidence, not the digital image itself, digitally signed, and authenticated by an expert witness in court. The examples of such condition were shown in *Gorgonia v Argubi*

⁶¹ Law No. 11 of 2008, Article 1 Para. 1.

⁶² Law No. 11 of 2008, Article 5 Para. (2), Code of Procedure meant under this Article is Indonesia, Law No. 8 of 1981 on the Code of Criminal Procedure (State Gazette 1981 No. 76).

⁶³ Law No. 11 of 2008, Article 5 Para. (3).

⁶⁴ Indonesia, Government Regulation No. 71 of 2019 on the Administration of Electronic System and Transaction (State Gazette 2019 No. 185), Article 1 Para. 1.

⁶⁵ GR No. 71 of 2019, Article 1 Para. 4, 5, and 6.

⁶⁶ GR No. 71 of 2019 Article 1 Para. 22.

⁶⁷ District Court of Dumai, “Decision No. 27/Pdt.G/2012/PN.DUM”, 57-59.

⁶⁸ District Court of Dumai, “Decision No. 9/Pdt.G/2017PN.DUM”, 10.

*Mendan*⁶⁹ where, in another land dispute, the respondent submitted a photocopy of a satellite image to the supposed location of the land in dispute, without authentication by an expert witness, nor producing the digital data with proper digital signature or producing any certified true copy of the image. The cases of *Saddiah v Sausia & Sulastra*,⁷⁰ also shown similar trends of submitting non-certified copies of an earth observation image.

Aside from land disputes, some criminal cases in Indonesia also utilized earth observation data as evidence in court. In *Rusma Yul Anwar Case*, imaging data produced by a Pleiades Satellite was used in an environmental case where the defendant demolished a Mangrove Forest he owned, which has been designated as protected areas.⁷¹ In this case, the data was authenticated by the National Geospatial Bureau in 2016 and was used by the expert witness in mangrove forests as part of his testimony.⁷² In another environmental criminal case, a district court refused to accept earth observation data as evidence presented by an expert witness in *Adat Law*, due to lack of expertise and incomplete real data used while interpreting the image.⁷³

Based on observation of the aforementioned cases, it can be seen that the lack of proper procedural basis for authentication of electronic data to be used as evidence in court proceedings, provides an unclear way to admitting such data, and opening a possibility for misuse or misrepresentation of such data in court. Although, there are also some cases that the court requesting a form of authentication in using or in analyzing data obtained from earth observation satellites.

C. The Americas

In the Americas, particularly in the United States, the primary basis to submit EO Data as evidence lies in the *Frye Rule*,⁷⁴ which stipulates that in submitting scientific data as evidence, a general acceptance needs to be made by the court to a new scientific method to obtain data that is produced within a sound, scientific methodology.⁷⁵ In a recent development, however, there is another rule, the *Daubert Rule*,⁷⁶ which stipulates that a general acceptance of new scientific methods in producing evidence, need not exist prior to submission of data as evidence, so long as this data was produced with *scientific validity*.⁷⁷ Hence, from a scientific point of view, it can be said that the US has acknowledged that EO data, when treated as scientific evidence, may be admissible, as long as it is scientifically valid and reliable. From a digital or electronic evidence point of view, the US has precedent in using satellite data as evidence in court. In *U.S. v Bennett*,⁷⁸ GPS Data was used in an immigration case, which although not using EO Data, this case is relevant as precedent for cases that use satellite data as evidence.⁷⁹ As for its Federal Rules of Evidence, in the

⁶⁹ District Court of Tanjung Selor, "Decision No. 15/Pdt.G/2019/PN.TJS", 29.

⁷⁰ District Court of Kendari, "Decision No. 14/Pdt.G/2019/PN.KDI", 8.

⁷¹ District Court of Padang, "Decision No. 642/Pid.Sus-LH/PN.PDG", 8.

⁷² Decision 642/Pid.Sus-LH/PM.PDG, 116.

⁷³ District Court of Muara Teweh, "Decision No. 148/Pid.B/LH/2019/PN.MTW", 30.

⁷⁴ *Frye v U.S.*, 293 F. 1013 (D.C. Cir 1923)

⁷⁵ Susan Rae Wolfinbarger, *People Make the Pixels: Remote Sensing Analysis for Human Rights-Based Litigation* (2012), 51.

⁷⁶ *Daubert v Merrell Dow Pharmaceuticals Inc.* 509 U.S. 579, 113 S.Ct. 2786 (1992).

⁷⁷ Wolfinbarger, *People Make*, 52.

⁷⁸ *U.S. v Bennett* 363 F.3d 947 (9th Cir. 2004).

⁷⁹ Leah Voigt Romano, "Electronic Evidence and the Federal Rules," *Loyola of Los Angeles Law Review* 38 (2005): 1746.

beginning, Section 901 stipulates that any electronic evidence submitted must have a digital signature and authentication by an expert witness in court.⁸⁰ However, in another recent development, the US took a different approach in the authentication of digital evidence, to which it does not require an expert witness to be present in court to authenticate electronic evidence and makes electronic evidence, with a digital signature that is properly produced, self-authenticating.⁸¹ This opens a big opportunity in submitting EO data as electronic evidence and may create new precedents in US case laws.

V. CONCLUSION

From the matters presented by this paper, it is shown that the utilization of EO data as evidence in legal proceedings is not without issues. A proper procedure to ensure the accuracy and authenticity of the data needs to be established. The process of data imaging and digital signature is the best way to achieve this, mainly because EO data is digital data, be it in form of image or sensor information. However, for the data to be considered usable as evidence, it has to have a clear chain of evidence, not just merely using the processed, publicly available data as evidence. This can be achieved by making both the raw data and the processed data available to be used digitally for forensic purposes. There are several ways for Sensed States to be able to gain this EO data for evidential purposes. The current regime is to obtain evidence through the MLA agreement. But this agreement is naturally focused more on criminal law matters, rather than giving way to civil or administrative law proceedings. Another way for States to obtain the entire chain of data is through an ISTA Agreement. However, the existing ISTA between a Sensing State with a Sensed State only allows remote sensing capabilities or data obtained for scientific purposes. Hence, although Sensed States have access to EO data with this agreement, a proper process to use the same EO data for legal proceeding purposes. From the availability point of view, there has to be legal development to make EO data easily obtained by all Sensed States, in order to make sure that space capabilities can support the establishment of Rule of Law. An example of the agreement for future legal development in the utilization of EO data as evidence in court proceedings can be taken from the Evidence Convention, especially for using EO data in civil or commercial disputes.

Based on the findings made, this paper moves to recommend that there has to be an amendment to the UN Principles on Remote Sensing, to accommodate its use other than environmental protection or disaster mitigation, to avoid liberal interpretation of these principles. There also must be special guidelines and standards internationally on how to treat this EO data as evidence in legal proceedings, with the basis of current existing electronic evidence regimes in various jurisdictions. In terms of availability, the Sensing States has to open more opportunities for the Sensed States, and disputing parties in the Sensed States, to obtain EO data for their legal needs, not just for scientific purposes. A model agreement that encompasses various use of this data may be created to accommodate this issue. Nationally, an ample procedural law must be established to authenticate earth observation data to make it admissible as evidence in court proceedings.

⁸⁰ Carl A. Aveni, "New Federal Evidence Rule Changes Reflect Modern World," accessed April 15, 2020, <https://www.americanbar.org/groups/litigation/publications/litigation-news/featured-articles/2018/new-federal-evidence-rule-changes-reflect-modern-world/>.

⁸¹ Aveni, "New Federal"

BIBLIOGRAPHY

Books

- Ito, Atsuyo. *Legal Aspects of Satellite Remote Sensing*. Leiden: Brill, 2011.
- Wagner, Caroline S. *International Agreements on Cooperation in Remote Sensing and Earth Observation*. Washington D.C.: RAND, 1998.
- Purdy, Ray and Denis Leung. *Evidence from Earth Observation Satellites: Emerging Legal Issues*. Leiden: Brill, 2013.
- van Rhee, C.H. *Evidence in Civil Law – The Netherlands*, 2012.
- Wolfenbarger, Susan Rae. *People Make the Pixels: Remote Sensing Analysis for Human Rights-Based Litigation*, 2012.
- Masson-Zwaan, Tanja and Mahulena Hofmann. *Introduction to Space Law*. Alphen Aan den Rijn: Kluwer, 2019.

Articles

- Arzt, Clemens. "Use of Satellite Imagery in Legal Proceedings." *Air and Space Law* 24 (1999): 196.
- Bonnici, J.P. Mifsud *et al.* "The European Legal Framework on Electronic Evidence: Complex and in Need of Reform." In *Handling and Exchanging Electronic Evidence Across Europe*, ed. M. A. Biasiotti, J. P. Mifsud Bonnici, J. Cannataci, and F. Turchi, 2018.
- de Busser, Els. "The Digital Unfitness of Mutual Legal Assistance." *Security and Human Rights* 28 (2017): 164.
- Doldirina, Catherine. "Open Data and Earth Observations: The Case of Opening Up Access to and Use of Earth Observation Data Through the Global Earth Observation System of Systems." *Journal of Intellectual Property, Information Technology, and E-Commerce* 73 (2015): 75.
- Friederich, Brian. "Reinforcing the Hague Convention on Taking Evidence Abroad after Blocking Statutes, Data Privacy Directives, and Aerospatiale." *San Diego International Law Journal* 12, No. 1 (2010): 273.
- Hufstetler, Kristopher R. "The Admissibility of Aerial Photographs - Evidentiary Foundations", *St. Mary's Law Journal* 47 (2016): 860.
- James, Joshua I. and Pavel Gladyshev. "A Survey of Mutual Legal Assistance Involving Digital Evidence", *Digital Investigations* 18 (2016): 24.
- Markowitz, Kenneth J. "Legal Challenges and Market Rewards to the Use and Acceptance of Remote Sensing and Digital Information as Evidence." *Duke Environmental Law & Policy Forum* 12 (2002): 236.
- Mckemmish, Rodney. "When is Digital Evidence Forensically Sound?" In *Advances in Digital Forensics IV*. Ed. Indrajit Ray and Sujeet Shenoj (2008): 5-6.
- Romano, Leah Voigt. "Electronic Evidence and the Federal Rules." *Loyola of Los Angeles Law Review* 38 (2005): 1746.
- Wang, Ningna and Rujun Yang. "The Application of Chinese High-Spatial-Resolution Remote Sensing Satellite Image in Land Law Enforcement Information Extraction." *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences* 42 (2018): 1751.
- Vettorel, Ariana. "Global Positioning System Evidence in Court Proceedings and Privacy: The Case of Italy." *Air and Space Law* 42 (2017): 297.

Legal Documents

- Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters*, UN Treaty Series Vol. 847 No. 12140. (1970).
- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, UN Treaty Series Vol. 610 no. 8843. (1967)
- UN Principles on Remote Sensing*, UN Res 41/65 of 3 December 1986.
- European Council, *Guidelines for Electronic Evidence in Civil and Administrative Proceedings* (2019).
- Indonesia, *Law No. 11 of 2008 on Electronic Information and Transaction* (State Gazette 2008 No. 58).
- Indonesia, *Law No. 19 of 2016 amending the Law No. 11 of 2008 on Electronic Information and Transaction* (State Gazette 2016 No. 251).
- Indonesia, *Government Regulation No. 71 of 2019 on the Administration of Electronic System and Transaction* (State Gazette 2019 No. 185).
- District Court of Dumai, "Decision No. 27/Pdt.G/2012/PN.DUM".
- District Court of Dumai, "Decision No. 9/Pdt.G/2017PN.DUM"
- District Court of Kendari, "Decision No. 14/Pdt.G/2019/PN.KDI"
- District Court of Muara Teweh, "Decision No. 148/Pid.B/LH/2019/PN. MTW"
- District Court of Padang, "Decision No. 642/Pid.Sus-LH/PN.PDG"
- District Court of Tanjung Selor, "Decision No. 15/Pdt.G/2019/PN.TJS".
- UK Association of Chief Police Officers, *Good Practice Guide for Digital Evidence* (2012)
- UK Parliamentary Office of Science and Technology, *Digital Forensics and Crime*, 520 Postnote (2016).
- Cheng Swee Tiang v PP*, MLJ 291 (1964).
- Daubert v Merrell Dow Pharmaceuticals Inc.* 509 U.S. 579, 113 (S.Ct. 2786 1992).
- Frye v U.S.*, 293 F. 1013 (D.C. Cir 1923)
- U.S. v Bennett* 363 F.3d 947 (9th Cir. 2004).

Websites

- Aveni, Carl A. "New Federal Evidence Rule Changes Reflect Modern World." Accessed April 15, 2020. <https://www.americanbar.org/groups/litigation/publications/litigation-news/featured-articles/2018/new-federal-evidence-rule-changes-reflect-modern-world/>.
- Macauley, E.D. "The Role Satellites Should Play in the Protection and Promotion of Human Rights, Including the Use of Earth Observation Satellites in Evidential Matters." Accessed April 13, 2020. https://www.mcgill.ca/iasl/files/iasl/wef-mcgill_space-macauley.pdf.
- NASA. "Data Processing Levels." Accessed April 5, 2021. <https://earthdata.nasa.gov/collaborate/open-data-services-and-software/data-information-policy/data-levels>.