International Conference on Business Economics, Social Sciences & Humanities

Analysis of United States Cyberpower Domination through the Cloud Act on Data Security in Europe

D Triwahyuni[1], Y W Nugraha[2], I R H Permana [3], Z A Falentino [4]
[1,2,3,4]Department of International Relations, Universitas Komputer Indonesia, Indonesia, Jl. Dipati Ukur No.112-116, Bandung, Indonesia
[1]dewi.triwahyuni@email.unikom.ac.id,[2]yudha.44319031@mahasiswa.unikom.ac.id,
[3]igna.44319030@mahasiswa.unikom.ac.id, [4]zahra.44319026@mahasiswa.unikom.ac.id

Abstract. This study aims to analyze the dominance of US cyberpower through the Cloud Act on data security in Europe. Currently, the business of storing and processing data via a network, commonly known as the cloud, is dominated by US technology giants. Meanwhile in Europe, business people and governments failed to reach an agreement to form a cloud service to match that dominance. One of the causes of European concern is the law in the US called the Cloud Act. This agreement provides for complying with their obligations to store, back up, or disclose electronic data in their possession regardless of where that information is located. That way, the United States can have special access to be able to access state data without the need for a warrant. The research method used is descriptive qualitative with data collection techniques through interviews, documentation, and literature study from books and e-journals. Determination of informants using purposive sampling method. the validity and reliability of the data were tested using data triangulation techniques. The results of the analysis in this study show the dominance of US cyberpower in the global cloud system business. The conclusion of this study is that it is very important to build readiness in facing the onslaught of American cyber power dominance starting from setting regulations that can be agreed upon by the international community by prioritizing technological modernization so that every country has the same opportunity to build and secure its own cloud system**.**

1. Introduction

The Cloud Act is a US law that was approved in 2018. It outlines how US law enforcement agencies and technology companies should handle data stored in the cloud. The law provides clarity on the jurisdiction of US law enforcement over data stored by US-based companies, regardless of where the data is physically stored. The Cloud Act was created due to the rapidly evolving technology and the growing use of cloud computing. As more personal and business information was being stored in the cloud, concerns about privacy, security, and access to the data by law enforcement agencies were on the rise. This law was also created in response to a case where the US government sought access to data stored by Microsoft in Ireland for a criminal investigation. This case raised questions about the jurisdiction of US law enforcement

over data stored abroad and the Cloud Act aimed to resolve this issue by clarifying the jurisdiction of US law enforcement over data stored by US companies, regardless of its location.

The Cloud Act was seen as a necessary step to ensure that law enforcement agencies had the necessary tools to carry out investigations and to prevent criminal activity, while also protecting the privacy and security of citizens and businesses. The act has been widely recognized as an important step forward in balancing privacy and security in the digital age.In terms of cybersecurity, the Cloud Act is important because it establishes the responsibilities of cloud service providers to protect customer data, and it also lays out the procedures for government agencies to access this data. This act helps to balance privacy and security concerns, as it sets out clear rules for how data can be collected, used, and protected.

The main purpose of this agreement known as the CLOUD ACT is divided into 2 main points main points. The first point is to change the storage of communication data to the provider communication service providers can comply with the conditions for storing, backing up or disclose electronic data held by the communication service provider regardless of where the information is located and where it goes. the information is located and where it goes. The second point is that it is prohibited the United States Government from having access with governments bound for reciprocal access expedited feedback to electronic information held by a communications service provider based overseas. communications service providers based overseas. (1)

The term "data security" encompasses the strategies and procedures implemented to safeguard sensitive and confidential information from unauthorized access, usage, disclosure, destruction, alteration, or disruption. Data security is a critical issue in today's digital era, because there are more and more of them personal and business data is being stored, processed, and transmitted electronically. This data can include sensitive information such as financial records, personal identification numbers, medical records, and confidential business information. There are many threats to data security, including hacking, phishing, malware, and theft of devices containing sensitive information. To address these threats, organizations and individuals must take steps to secure their data. This can include implementing strong passwords, using encryption technologies, and regularly backing up data to prevent data loss in the event of a security breach.

Organizations must also implement policies and procedures to ensure the secure handling of sensitive information, including strict access controls, monitoring of network traffic, and regular security audits. It is also important for organizations to stay informed about the latest security threats and technologies, and to regularly review and update their security measures. In addition to these technical measures, data security also requires a strong culture of security awareness, in which all employees understand the importance of protecting sensitive information and take the necessary steps to ensure its security. This includes being vigilant about phishing attempts, being careful when working with sensitive information, and reporting any suspected security breaches.

Data security is an ongoing process that requires ongoing attention and investment. By taking a proactive and multi-faceted approach to data security, organizations and individuals can protect themselves against security threats and maintain the privacy and confidentiality of their sensitive information. In the Black's Law Dictionary, A treaty between two or more independent states. Brendi contract, a bond agreement between two or more states or sovereigns signed by commissioners authorized and solemnly ratified by the various sovereigns or supreme powers of each state. (2)

The Cloud Act, a legislation passed in the United States, has had a significant effect on data privacy and security in Europe. The law grants US law enforcement agencies the power to access data held by US companies, regardless of its location, even if it is stored outside the country, for instance in Europe. This has sparked worry among privacy advocates in Europe, who claim that the law undermines the privacy rights of EU citizens. To counteract the impact of the Cloud Act, the European Union has taken steps to fortify its own data protection framework. Specifically, the EU has enacted the General Data Protection Regulation (GDPR), which establishes stringent guidelines for the collection, handling, and storage of

personal data. Additionally, the GDPR gives EU citizens the right to request that their personal data be erased and to be notified when their data is being processed.

The GDPR has had a significant impact on U.S. companies operating in Europe, as they must now comply with the strict privacy and security requirements of the regulation. This has led to calls for the U.S. to adopt similar privacy and security standards, in order to ensure that the privacy rights of EU citizens are protected when their personal data is stored and processed by U.S. companies. In conclusion, the Cloud Act has led to increased concern about the protection of personal data in Europe, and has led the EU to take steps to strengthen its own data protection framework. The GDPR has had a significant impact on U.S. companies operating in Europe, and has prompted calls for the U.S. to adopt similar privacy and security standards.

The major formulation of the problem in data security within the European Union (EU) through Cloud Act can be summarized as follows: Increasing amounts of personal and sensitive data being collected, processed, and stored electronically, With the growth of digital technologies, there is an increasing amount of personal and sensitive data being stored and processed electronically, which presents significant security risks. Threats to data security: The increasing amount of data being stored and processed electronically has led to an increase in the number and sophistication of security threats, including hacking, phishing, malware, and theft of devices containing sensitive information. Weaknesses in current data security measures: Many organizations and individuals have not taken adequate steps to secure their data, leaving it vulnerable to security threats. There are also weaknesses in the current data security measures being used, including weak passwords, unencrypted data, and the lack of regular security audits. Inadequate implementation of data protection regulations: Despite the implementation of the General Data Protection Regulation (GDPR), there are still concerns about the inadequate implementation of data protection regulations within the EU, which has led to ongoing privacy and security risks. Lack of harmonization of data protection laws across the EU: There are different data protection laws across the EU, which can create confusion and make it difficult for organizations to comply with the regulations. This can also make it more challenging for the EU to enforce data protection regulations and ensure that EU citizens' privacy rights are protected.

These are the major formulation of the problem in data security within the European Union, which must be addressed in order to ensure the protection of sensitive and personal data in the digital age. In addition to the major formulation of the problem in data security within the European Union, the Cloud Act has also raised several minor problems related to data security: Conflicts with EU data protection laws: The Cloud Act has raised concerns about its compatibility with EU data protection laws, as the act allows U.S. law enforcement agencies to access data stored by U.S. companies, regardless of where that data is stored, including in the EU. This has led to concerns about the potential for U.S. law enforcement agencies to access EU citizens' personal data without their consent.Lack of transparency: The Cloud Act has been criticized for its lack of transparency, as it allows U.S. law enforcement agencies to access data stored by U.S. companies without informing the individuals whose data is being accessed. Lack of legal recourse: EU citizens whose personal data is accessed under the Cloud Act have limited legal recourse, as the act is a U.S. law and is not subject to EU data protection regulations. Uncertainty about the security of data stored by U.S. companies: The Cloud Act has raised concerns about the security of data stored by U.S. companies, as there are questions about the safeguards in place to prevent unauthorized access to personal data..

A previous study that highlighted the cloud act agreement was conducted by Alessandro Praputranto and Jun Justinar (2022). They highlight how humanitarian law responds to treaties cloud *act*, they consider that the creation of an agreement based on the Cloud Act is a new breakthrough and brings various kinds of benefits to the security and defense of the country. Moreover, in humanitarian law that believes in the principle of military interests, the principle which states that in the management of state defense and security, military interests are prioritized over individual and group interests. (3)

Meanwhile, another study tries to explain how far the Cloud Act seeks to clarify the extent to which the US and foreign governments can access user data stored by US-based communication service providers, during a criminal investigation. Study conducted by Halehom H. Abraha (2019).

While research conducted by Muh. Firmansyah Pradana with the title Legal Protection Against Users*Cloud Computing* On Privacy and Personal Data (2018) where the author examines the concept of regulation of privacy and protection of personal data in the system cloud *computing*, focuses on the contents of the agreement between service providers cloud *computing* related to the rights and obligations of service providers, users or customers. (5)

Also research with the title *"21 Thoughts and Questions about the UK-US CLOUD Act Agreement (and an Explanation of How it Works – with Charts)"* by Theodore Christakis (2019). They highlighted how the process of UK-US relations was intertwined through the Cloud Act Act agreement. (6)

Last, research from Jordan A. Klumpp entitled International Impact Of The Clarifying Lawful Overseas Use Of Data (Cloud) Act And Suggested Amendments To Improve Foreign Relations (2020) which highlights the impact of international use of data abroad and this research seeks to provide suggestions on how changes can improve relations between foreign countries through the UUD Cloud Act agreement. (7)

By using Case Study Research with the method that involves in-depth analysis of a single case or small number of cases to gain insights into a particular phenomenon which is the issues of Cloud Act in European. Researchers typically use a variety of data sources with amount of reference from another research that collected with hope that any recent or past studies can relate and find another solution to this topic, also including interviews, observations, and document analysis, to develop a detailed understanding of the case.

2. Research Methods

This journal article employed a qualitative research methodology that relied heavily on the interpretation of data and sources collected from existing literature relevant to the topic being studied. The research utilized a descriptive qualitative approach, utilizing data collection techniques such as interviews, documentation analysis, and a review of books and electronic journals. The informants were selected through a purposive sampling method. The validity and reliability of the data were assessed using triangulation techniques.

This research focuses on describing the situation of the European Union in dealing with this Cloud Act agreement and how the impact and actions will be taken based on data security policies in the European Union. This research also provides an overview of the state of American cyber power in dominating cloud computing systems because this policy provides authority to law enforcers to act beyond jurisdiction across national borders.

Literature studies are used in finding credible and valid sources by collecting relevant journals to be studied according to the goals to be achieved. and literature studies obtained from internet sources and university libraries. Therefore, literature on cyber security and its theories regarding cyber power to be able to assess how America dominates in this case.

3. Discussion

3.1 How's The CLOUD Act are Formed

An arrangement between multiple nations or entities, also known as a bilateral treaty, has existed since the year 1969. In general, the agreement is made based on international law which is intended to regulate the rights and obligations of each party. Of course, to make an agreement that involves not only one country or international level, it is necessary to have a convention as a basic guideline for its provisions.

The convention that is considered to be the parent of all agreements is the Vienna Convention. The convention contains provisions governing international treaty matters. According to the Big Indonesian Dictionary, an agreement is an official agreement between two or more countries which contains matters relating to security, trade, and so on. In Article 2 paragraph (1) letter a of the 1969 Vienna Convention, international agreements are: "International agreements are signed in writing between countries and governed by international law, whether contained in one document or in two or more documents, and regardless of their title" Based on this understanding, it can be concluded that the agreement is an agreement or agreement that is official, which involves two or more countries which contains the fields of international standard state interests in the form of ratification by the authorities and sovereign. itself is not only limited to agreements that are obliged to promise. International agreements themselves can be agreements that include agreements from contracts, charters, protocols, conventions, cooperation that give rise to international agreements and others. Usually agreements are born in the form of clauses codified in a piece of paper d and stored in a visible physical form. Over time, the development of science and technology (IPTEK) has progressed rapidly. Agreements that were previously made by typing or writing on a piece of paper were then codified after direct ratification, now there is no need for conventional ratification. Advances in science and technology provide new breakthroughs in cloud computing that can store contract data or file other cloud-based database storage. With the enactment of a data-based cloud or cloud database, now agreements no longer have to be made in the traditional way. As an example of the realization of an agreement that uses a cloud-based system today, namely the superpower, the United States, invites Northern Ireland and Great Britain to work together to implement the benefits of civilization and science and technology progress in an international agreement called the Cloud Act. The provisions regarding international agreements in the Cloud Act contained in article 2 of this Cloud Act discuss the purpose of this agreement.

The emergence of electronic data agreements that provide freedom for countries bound by the Cloud Act agreement is a form of civilization resulting from the development of science and technology. Of course, each development has advantages and disadvantages. It should be noted that in addition to bringing many advantages, based on this cloud-based agreement also brings a myriad of potential problems that must be addressed first. One of the problems that is of serious concern is the emergence of cyber wars which are very vulnerable to occur due to the opening of access by communication service providers. The security of a country is important and crucial. Because in the Cloud Act Act, with the existence of the agreement, the countries that are bound by the agreement must provide access to view the data stored on their cloud computing systems. The agreement is indeed intended to provide security and comfort, but at the same time it is a very serious threat to the security of the country concerned.

In the context of national security, Uncle Sam's country sees cyber or cyber security. This is a very important and vital thing to learn. Cybersecurity is a priority for the United States' domestic political policy considering its very vital existence. The United States government builds a network of information security systems in the military, agrarian, traffic management systems, water and sanitation, energy and transportation. This vital aspect is very dependent on the role of computers and cyberspace. Because of this, the United States government made updates to standardize cyber security.

Currently, the domination of US technology in the business of processing and storing data via digital networks commonly known as the Cloud is one of the things the European Union is concerned about. Meanwhile in Europe itself, they have failed to reach an agreement to form a Cloud service to match that dominance. Reporting from the geopits.com page, technology companies from America are ranked highest as the largest Cloud Database in 2023. Among them are Microsoft Azure SQL Database, Amazon Web Services (AWS), Google Cloud Spanner. Large German companies such as automotive giant Volkswagen (VW) for example use the service and store their data on Amazon Web Services. Meanwhile,

Deutsche Bank and Lufthansa use Google Cloud services. The French Ministry even chose Microsoft to store and process its research data.

3.2 The CLOUD Act definition

The CLOUD Act, short for Clarification of Lawful Foreign Use of Data Act, which means a federal legislation that became effective in 2018 within the United States. The law gives law enforcement agencies location independent access to electronic communications data stored in the cloud. The CLOUD law has sparked debate, with some arguing that it will affect privacy and civil liberties, particularly with regard to information held by foreigners. Supporters of the law argue that it is an important police tool for fighting crime and terrorism and balancing privacy and security interests. The CLOUD Act is a database cloud contract commonly referred to as cloud computing. Cloud computing is a combination of information technology and internet development. "Cloud" is another term for the internet or cyberspace, because clouds are often represented in computer network diagrams. In cloud computing, "cloud" is also an abstract representation of a complex invisible infrastructure. Internet Cloud is a computing model in which IT capabilities are offered as a service over the Internet (8).

The CLOUD Act is a trilateral agreement established between the United States, Ireland, and the United Kingdom. The main objectives of the agreement are twofold: Firstly, to modify the Stored Communications Law and enforce Internet service providers to fulfill their responsibility to store, secure, or release electronic data from any location; and 2) allow the US government to enter into implementation agreements with foreign governments for shared, offshore access to electronic information maintained by service providers outside the country. This historic agreement will significantly speed up investigations and help police protect the public from serious crimes. At the same time, it is hoped that the confidentiality and security of the personal data concerned is maintained.

The impact of the CLOUD Act is undeniable. Quick access to information is essential, as shown by the fact that the UK and Australia have enacted similar laws. Most of the world's data is stored in the United States, so waiting times to obtain electronic evidence from American providers is a major hurdle for foreign investigators. This has prompted other countries to increase protections for privacy and civil liberties.

The first section, now codified in 18 USC § 2713, states that providers of electronic communications services or remote computing services must comply with chapter obligations regarding recorded wired and electronic communications. "Whether the news, documents or other information is located inside or outside the United States." The three governments agreed to provisions that largely lifted restrictions on full investigations, did not target residents of other countries, and ensured ISPs that data disclosure agreements complied with their user privacy laws. The parties to the agreement also promise to obtain permission from other countries before using the information obtained through the agreement in police activities related to the vital interests of the party, especially in the prosecution of capital punishment in relation to matters regulated by law.

Several groups have expressed concern about the potential harm this agreement could cause to privacy and human rights, arguing that the CLOUD agreement undermines "individual rights both within and outside the United States." The agreement not only reviews and applies other countries' domestic laws with regard to "adequate protections of privacy and civil liberties," but also limits who Americans can target, including individuals inside and outside the United States.

The purpose of this agreement is to resolve potential legal conflicts that communication service providers may face when asked to provide electronic information. The agreement covers several countries and assesses the suitability of each country to participate, e.g. B. Adequate legislation on cybercrimes and electronic evidence, respect for human rights, and clear powers for government agencies. In addition,

participants must comply with the restrictions on the use of resources in the agreement and also respect the privacy of their own country. This is explained in Article 9 paragraphs 1 and 2 of the agreement.

An explanation of the provisions of US federal laws should begin by explaining the legal challenges that led to the creation of those laws. The rapid growth of cloud computing, which provides people around the world with access to services such as social media, email, file storage and media streaming, is due to the ability to process large amounts of data based on virtualized IT resources. in a different place. data centers around the world. Known as software-as-a-service (SaaS), these services are highly scalable, partly due to the separation of infrastructure and application layers. This allows, for example, email open requests to be served by application servers located in different data centers in different countries, in which case the term "data localization" is difficult to define in cloud services. Distribution of user data is determined by algorithms aimed at improving service availability, and these cloud services operate across borders and often around the world. In the past, many SaaS contracts entered into with European users included a clause stating that US law would apply. With the entry into force of Regulation 2016/679, major CSPs such as Microsoft, Google, Facebook and Yahoo had to change their service rules to allow their European subsidiaries to enter into agreements with users and thereby become data controllers under EU regulations. But technically, these services are not provided by one company, but by several related companies belonging to the same capital group. Responsibility for ensuring service provision, d. H. Technical management of IT infrastructure in on-site data centers should be separate from the role of service provider, ie. user. The two functions can be the same or different parties. For example, Google has several data processing centers in the EU managed by different companies, but all contracts with EEA users are managed by one entity, Google Ireland Ltd. Such information may be requested as part of an ongoing criminal case.

Federal law establishes specific protocols for seeking disclosure that vary by jurisdiction and the type of information involved. It is very important to distinguish between electronic communication services and remote computing services. For cloud storage services, the access status may change depending on the data stored or transferred. Federal law places various requirements on government agencies regarding the availability of data collected and transmitted using electronic communications services and remote computing services. Because of the broad definition of an official entity, US law enforcement agencies (LEA) have requested information not only when those entities physically possess the information, but also when they are monitoring information stored on servers overseas, even if they do not have it. he. they do not have direct access to the data. An example is the SCA license granted to Microsoft Corporation in 2013, which required it to provide data in criminal proceedings. Microsoft must provide information collected from certain email accounts, including email content, within 14 days. The company discovered that some of the data, except for the email content, is stored on servers in the United States, but the email content is stored overseas. This would require cross-border data transfers to US leaders, circumventing local regulations and risking violating national regulations. Microsoft took legal action to overturn the order, and the dispute later went to the US Supreme Court. This case led to the passage of the CLOUD Act in 2018 to clarify US law enforcement's access to electronic evidence owned or controlled by US companies but stored in foreign databases. The federal parliament supports a hybrid model in which national legal norms are supplemented by voluntary international agreements with third countries. In the process of drafting the new law, legislators also introduced mechanisms to challenge national data disclosure orders that could result in violations of mandatory foreign jurisdiction standards.

4. Result

4.1 The U.S Law Enforcement Access to Foreign Data

Among the "conventional findings" included in the CLOUD Act was the assertion that the US government's efforts to obtain timely electronic evidence were hampered by the inability to access data stored outside the state. The law responded to this challenge by amending the Stored Communications Act

(SCA), which has been criticized for years as outdated and not up-to-date. Among other things, a new provision in Chapter 121 of Title 18 of the Code America Union requires service providers to provide customers with their data to US authorities, wherever they are located.

This provision clarifies two main issues - jurisdiction over mail search orders issued under SCA and governing jurisdiction over data stored from foreign servers - which were also important in the case of Microsoft Ireland. In the latter case, Microsoft's main argument is based on the presumption of extra-territoriality, which it argues is jurisdiction based on physical location data. The CLOUD Act solves this problem by regularly allowing US law enforcement agencies to compel service providers to send data stored overseas. In other words, in a situation like Microsoft Ireland, the jurisdiction of the test is the information requested is "controlled, owned, or controlled" by the US service provider, not where the information was requested. As long as the service provider is a US company, it doesn't matter if the requested information is stored inside or outside the US. In other words, US service providers cannot circumvent US government access by simply sending data out of the country. “Ownership, maintenance or control” is not within the scope of this chapter, but will generally depend on the general situation determining the practical ability or right of the legal provider to obtain the information requested. Lagging behind best efforts, the CLOUD Act addresses two important aspects of the definition of "ownership, custody, or control" in the context of cloud services. First, US service providers may override effective data management to circumvent US jurisdiction, and the law does not effectively address this issue on a regular basis. This is not just a theoretical possibility, as Microsoft has adopted a "data custodian" model, placing data customers outside the jurisdiction of the US government through partnerships with foreign companies Microsoft announced in 2015 that it would entrust Deutsche Telekom with responsible answers for its German data centres. While the EU's data protection model is often widely regarded as the most comprehensive in the world and a model for other lawmakers, it cannot be ignored that its applicability to other legal systems has increased. The Lisbon adoption reform raises questions about the EU's model of applying data protection, believed to be the most comprehensive in the world, for other legal systems. For example, is the agreement between Microsoft and T-Systems, a subsidiary of Deutsche Telekom, whereby Microsoft delegates cloud data management to T-Systems customers as "official". Customer Does not have to terminate the contract with Microsoft, but with T-Systems. This creates a situation where the personal information of US persons needed for domestic research into US crimes may not be in the US or not regularly controlled effectively by US companies. Some believe that this step was intended by Microsoft to avoid a repeat of the US-Microsoft incident. Because Microsoft has no legal right or practical ability to access data stored under this agreement, tests of ownership, retention, or control may not occur in practice. While a scalability model that Microsoft remains to see, this presents a potential challenge to the effectiveness of the CLOUD Act.

One of the biggest drawbacks of the CLOUD Act is the lack of clarity in determining Who is subject to mail order lookups in cloud-layered service settings. computing often involves complex agreements between multiple service providers, making it difficult for law enforcement agencies to identify the entity handling the data they find. This can result in CLOUD laws targeting service providers who do not actually own the data, creating a conflict between the law and the reality of cloud computing. In response to these concerns, the proposed EU regulations on production and storage rules offer some useful insights. In addition, product orders may be sent to key infrastructure service providers only in rare cases where research directed at the company or customer may be compromised.

4.2 The U.S.A’s Cyberpower analysis on CLOUD Act

Power and authority of the US government to access information held by companies outside the US. Compliance with the Lawful Use of Data Clarification Act (CLUD) is critical because it allows US law enforcement agencies to request access to this data. These permissions are granted regardless of the laws of other countries, including the European Union (EU), which have raised privacy and security

concerns in the EU. According to the Electronic Frontier Foundation (EFF), a non-profit organization focused on defending civil liberties in the digital world, the CLOUD Act "creates a new mechanism for foreign law enforcement agencies to request information from American companies, thereby violating privacy laws and due process protection is avoided in other countries." another."

The United States recognizes the importance of cybersecurity to national security and considers it an important issue to consider. As reliance on technology increases, digital security has become a top priority for US domestic policy. The US government has established information security networks in sectors such as the military, agriculture, traffic control, water and sanitation, energy and transportation, all of which rely heavily on computers and the Internet. As a result, the government is working to improve its cybersecurity standards. Additionally, the CLOUD Act provides impunity for companies that comply with US legal requirements, strengthening the US government's authority in this area. The EFF noted that this immunity "undermines the privacy protections of users around the world, including in the EU". to the US and expressed concern about privacy and security in the EU. This information comes from research and testing by the Electronic Frontier Foundation. The US government is building a network of information security systems across the military, agriculture, traffic control systems, water and sanitation, energy, and transportation sectors. These important aspects are very dependent on the role of computers and cyberspace. Because of this, the US government has updated its cyber security standards. (9)

The CLOUD Act (Clarification of Legal and Legal Use of Foreign Data) is a US federal law that was passed in 2018. The purpose of this law is to clarify the extraterritorial reach of US law enforcement agencies when using electronic data from companies located outside the US. (10)

The Cloud Act contains several main provisions, one of which is the clarification of powers. This section of the law makes it clear that US law enforcement agencies have the authority to access digital data from companies located outside the US, regardless of the physical location of the data or the location of the company. The CLOUD Act empowers the US government to enter into accords with foreign governments, which outline guidelines for law enforcement agencies on the appropriate usage of electronic data. The law further extends immunity to service providers who comply with requests from law enforcement agencies for electronic data, regardless of the location of the company or the storage location of the data. In addition, the CLOUD Act contains provisions to protect privacy when data is collected from abroad and to ensure that the data is used in accordance with the country's data protection laws. Essentially, the CLOUD Act strikes a balance between privacy requirements and enforcement by providing a framework for US law enforcement agencies to access electronic data held by foreign companies. (11)

4.3 EU Reaction Towards The CLOUD Act

The European Union (EU) has expressed concern about the extraterritorial reach of the CLOUD Act, as it conflicts with EU privacy laws and undermines the sovereignty of EU member states. The EU has also criticized the lack of privacy protections for European citizens in the act. In response, the EU has taken several steps to address these concerns. Example, The European Union strengthened its data protection laws with the General Data Protection Regulation (GDPR), which came into force in 2018. These regulations give individuals more control over their personal data and set strict guidelines that companies must follow when processing it. Personal information. (12) The European Union has aimed to negotiate bilateral accords with the United States to safeguard the privacy rights of EU citizens during cross-border transfers of electronic data. These agreements would create a structure for U.S. law enforcement agencies to access electronic data legally, while preserving the privacy laws of the EU. Additionally, the EU has also considered creating its own "cloud" initiative to provide European citizens with a safe and secure alternative to U.S.-based cloud services. This would help ensure that European citizens' personal data is protected and that the EU's privacy laws are respected. Overall, the EU's response

to the CLOUD Act reflects its concerns about the extraterritorial reach of U.S. law enforcement agencies and its commitment to protecting the privacy rights of European citizens (13).

Also, The European Union has various actions against the Cloud Act. Some of them are, Suspension of the EU-U.S. Privacy Shield: The EU suspended the Privacy Shield agreement with the U.S. in 2020, citing concerns about the U.S. government's ability to access European citizens' data under the Cloud Act. The Privacy Shield was a treaty established between the EU and U.S. to secure the privacy of EU citizens' data during transfers to the U.S. for business purposes. (14) Data Protection Regulations, The European Union introduced the Data Protection Regulation (GDPR) in 2018 as a measure to protect the personal data of EU citizens (15). Investigations into tech players,The European Union conducts investigations of big tech companies like Google and Facebook to ensure they comply with EU regulatory data.Fight against data threats: The European Union gives regulators the power to take legal action against companies that commit data theft. Data protection in trade, The European Union integrates data protection standards in its trade accords with other nations. Despite this, the Cloud Act has been met with criticism from the EU, with the union issuing a statement alleging that the Cloud Act conflicts with European Union data protection standards. These are just a few examples of the actions the European Union is taking against the Cloud Act virus and protecting the data privacy of EU citizens (16).

5. Conclusion

The conclusion of this research is that it is very important to build readiness in facing the onslaught of American cyber power domination starting from setting regulations that can be agreed upon by the international community by prioritizing technological modernization so that every country has the same opportunity to build and secure its own cloud system. the perception of the existence of a Cloud Act agreement that has an impact on the European Union which feels threatened by a cross-border privacy policy in which United States law enforcement is authorized to interrupt public data using cloud computing systems from America thereby resulting in conflicts regarding the power and power of American cyber in dominating the system cloud in Europe. In analyzing America's cyber power over the Cloud Act, we can conclude that America has significant power in terms of management and access to data stored in the cloud. The Cloud Act, which was implemented in 2018, gives American law enforcement agencies and technology companies the power to manage data stored in the cloud. This law asserts the jurisdiction of American law enforcement agencies over data held by American companies, regardless of the location where the data is stored. The importance of the Cloud Act can be seen from the rapid changes in technology and the increasing use of cloud computing. As the volume of personal and commercial data stored in the cloud increases, so do worries about privacy, security, and the capacity of law enforcement agencies to obtain that information. The introduction of the Cloud Act was a reaction to an incident in which the US government sought to retrieve information kept by Microsoft in Ireland for the purposes of a crime. This case raises questions about the jurisdiction of law enforcement agencies that do not have borders, where this is a concern for the European Union in maintaining the security of member countries' public data

References

[1] Center for Strategic and International Studies (2020). From https://www.csis.org/blogs/technology-policy-blog/cloud-act

[2] Black Law Dictionary 2nd Edition. (2014, February 25). What is TREATY? definition of TREATY (Black's Law Dictionary). The Law Dictionary. From https://thelawdictionary.org/treaty/

[3] Allesandro Praputranto & Jun Justinar (2022). Analisis Perjanjian Cloud Terhadap Potensi Perang Siber Dari Perspektif Asas Kepentingan Militer.

[4] Halehom H. Abraha (2019). How Compatitable is the US 'CLOUD Act' with cloud computing? A brief Analysis.

[5] Firmansyah Pradana, M (2018). Perlindungan Hukum terhadap Pengguna Cloud Computing atas Privasi dan Data Pribadi Legal Protection of Cloud Computing Users on Privacy and Personal Data. Tesis. Program Studi Magister Kenotariatan Fakultas Hukum Universitas Hasanuddin, Makassar, 42-47.

[6] Theodore Christakis (2019). *"21 Thoughts and Questions about the UK-US CLOUD Act Agreement (and an Explanation of How it Works – with Charts.*

[7] Jordan A. Klumpp (2020). judul International Impact Of The Clarifying Lawful Overseas Use Of Data (Cloud) Act And Suggested Amendments To Improve Foreign Relation

[8] The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, OJ C 306/1

[9] Triwahyuni, D., & Agustin Wulandari, T. (2016). *STRATEGI KEAMANAN CYBER AMERIKA SERIKAT. JURNAL ILMU POLITIK DAN KOMUNIKASI,* 6(1), 107–118. https://core.ac.uk/download/pdf/267935114.pdf Program Studi Ilmu Hubungan Internasional Universitas Komputer Indonesia, Program Studi Ilmu Komunikasi Universitas Komputer Indonesia

[10] Strite, A. S., & Morkoç, H. (1992). GaN, AlN, and InN: a review. *Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures Processing, Measurement, and Phenomena*, *10*(4), 1237-1266.

[11] Takeuchi, T., Sota, S., Katsuragawa, M., Komori, M., Takeuchi, H., Amano, H. A. H., & Akasaki, I. A. I. (1997). Quantum-confined Stark effect due to piezoelectric fields in GaInN strained quantum wells. *Japanese Journal of Applied Physics*, *36*(4A), L382

[12] The CLOUD Act. (2020, October 2). Center for Strategic and International Studies. Retrieved October 27, 2021, from https://www.csis.org/blogs/technology-policy-blog/cloud-act

[13] Biztech. (2020, August 18). Apa Itu Cloud Service Level Agreement? Retrieved February 12, 2023, from https://biztech.proxsisgroup.com/cloud-service-level-agreement/

[14] European Commission. (2020, July 16). EU-U.S. Privacy Shield: Commission suspends Privacy Shield and launches enforcement action against Facebook Ireland. Retrieved from https://ec.europa.eu/info/publications/eu-us-privacy-shield-commission-suspends-privacy-shield-and-launches-enforcement-action-against-facebook-ireland_en

[15] General Data Protection Regulation. (n.d.). Retrieved from https://gdpr-info.eu/

[16] U.S. Department of Commerce. (2020, July 16). EU-U.S. Privacy Shield: Suspension of the Privacy Shield Framework. Retrieved from https://www.privacyshield.gov/EU-US-Privacy-Shield-FAQs