LEGAL BRIEF
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 13, No. 5, 2024, pp. 1187-1193
Published by: IHSA Institute (Institut Hukum Sumberdaya Alam)

The Influence of International Law on the Enforcement of State Sovereignty Over Digital Resources

Wendy Budiati Rakhmi

Fakultas Hukum Universitas Pembangunan Nasional Veteran Jakarta

Abstract: This research examines the influence of international law on the enforcement of state sovereignty over digital resources, focusing on a comparison of digital sovereignty policies in the European Union, the United States and China. With the rapid development of technology and the increasing reliance on digital infrastructure, many countries have sought to strengthen their digital sovereignty to protect data, privacy and national security. However, the absence of comprehensive international legal instruments poses challenges in the fair and uniform enforcement of digital sovereignty. This research uses a qualitative-descriptive approach with a multiple case study method, analyzing legal documents, national policies, and reports of relevant international organizations to identify the impact of international law on digital regulation. The results show that the European Union places privacy rights as a priority by implementing the General Data Protection Regu-lation (GDPR), while the United States tends to support market freedom and technological innovation, but with some exceptions related to national security. China, on the other hand, takes a protectionist and centralized approach with strict control over data and digital access in its territory. In conclusion, these different approaches result in fragmentation in the management of digital sovereignty, which could threaten global connectedness. This research recommends international cooperation to create a global digital legal framework that balances state sovereignty rights with the need for connectedness and equitable access to data around the world.

Keywords: Digital Sovereignty; International Law; Data Privacy; Cyber Security; Digital Regulation

1. Introduction

The rapid advancement of information and communication technology in the 21st century has experienced many developments in various aspects of human life, including economic, social, political and legal aspects (Hamdan Mustameer, 2022; Wibawa, 2016). One of the most significant changes is the advancement of digital resources as a new form of wealth that not only has economic value, but is also strategic for the country. Digital resources include data, network infrastructure, data storage systems and digital platforms that become the main pillars in carrying out activities in various sectors, including economic governance and security (Buwono, Abubakar, & Handayani, 2022), (Ramayanti & Lubis, 2023). The issue of ownership, control and access rights to digital resources is becoming increasingly crucial, especially in the context of state sovereignty (Abimanyu, Setia, & Soegiharto, 2024), (Trio Andi, 2023). In the midst of digital globalization, states face challenges in maintaining their sovereignty in cyberspace. The concept of state sovereignty, which has focused on territorial and physical boundaries, is now beginning to shift and must take into account cyberspace as a new domain that needs to be regulated (Jihansyah, n.d.), (Purwantoro, 2023). However, the physical boundaries that are the main reference in international law are not always in line with the characteristics of the digital world that are global and cross-border (Syafi'i, Supriyadi, Prihanto, & Gultom, 2023), (Muslich, 2022).

This creates a dilemma in enforcing the law and state sovereignty over digital resources that are often spread across multiple territories and under the control of various

Correspondence:
Name: Wendy Budiati Rakhmi
Email: *wendy.budiati@upnvj.ac.id*

Received: Nov 07, 2024;
Revised: Nov 14 2024;
Accepted: Nov 22, 2024;
Published: Dec 30, 2024;

entities, including multinational corporations. International law has always played an important role in regulating relations between states, especially in matters of sovereignty, peace and security. However, the complexity and transboundary nature of digital resources raises new questions about the effectiveness of international law in regulating and protecting state sovereignty in the digital space (Gani, 2023), (Hamdan Mustameer, 2022). In recent years, efforts have been made to formulate globally acceptable rules and standards regarding the management of digital resources, such as data protection, cybersecurity and intellectual property rights in cyberspace (Adha, 2020), (Berlianti, Abid, & Ruby, 2024). However, international consensus on binding rules is still difficult to achieve due to different interests and perspectives between countries. Some of the established international legal instruments, such as the Budapest Treaty on Cybercrime and the Personal Data Protection Convention, only cover certain aspects of the management of digital resources in their respective territories (Sa'diyah & Vinata, 2016). As a result, many countries have begun to develop national policies to protect their digital sovereignty by regulating data ownership and control, adopting strict data privacy regulations, and controlling foreign access to critical digital infrastructure. A prime example is the data protection policy implemented by the European Union through the General Data Protection Regulation (GDPR) which seeks to protect the personal data of European citizens and empower member states to control digital resources in their respective regions. The existence of inadequate international law in addressing the issue of sovereignty over digital resources has led to various tensions between countries, especially between countries that have digital power and countries that tend to adopt protectionist policies to protect their digital resources (Nabila, Manabung, & Ramadhansha, 2024). On the one hand, developed countries that are leaders in digital technology, such as the United States and countries in the European Union, often promote policies that promote global access and management of data. On the other hand, many developing countries and countries with authoritarian governments see data as an important component of national sovereignty and adopt policies that restrict the flow of data abroad (Berlianti et al., 2024).

This has the potential to create internet fragmentation (splinternet), where each country has its own rules regarding data management and digital access, thus reducing global connectedness. In addition, the increase in cyber threats by both state and non-state actors adds a new dimension to the debate on digital sovereignty (Daniel, Shandi Negara, & Triadi, 2023). Cybercrime, digital espionage and attacks on critical infrastructure are a major concern for many states. In this context, existing international law is often insufficient to prosecute perpetrators in cyberspace, leading to a demand for the development of a more comprehensive international legal framework to regulate acts that threaten digital security and state sovereignty (Jl, Raya, Timur, Struktur, & Pedesaan, 2022).

This research seeks to examine the influence of international law on the assertion of state sovereignty over digital resources. This study is important given the state's increasing dependence on data and digital infrastructure in various aspects of life (Yuniarti & Herawati, 2020). In addition, this research seeks to identify the obstacles faced by states in maintaining their digital sovereignty amidst the fragmented and inconsistent dynamics of international law in addressing issues related to digital resource management (Hamdan Mustameer, 2022; Kristianto, 2022; Setiyawan, Churniawan, & Faried, 2020). Through a multidisciplinary approach that includes the perspectives of international law, cybersecurity and human rights, this research aims to provide a deeper understanding of the extent to which international law can support or hinder states in managing and protecting their digital resources. The results of this research are expected to form the basis for the development of more effective policies in balancing the state's need for digital sovereignty with the global interest in maintaining connectivity and cross-border data exchange.Materials and Methods

In this research, the approach used is a qualitative-descriptive approach with a multiple case study method to explore how international law plays a role in upholding

digital sovereignty in various countries (Setiyawan et al., 2020),(Berlianti et al., 2024). The case studies include digital policies and regulations in several countries, such as the European Union, the United States, and China, each of which has a different approach in managing sovereignty over digital resources. With this case study method, it is hoped that a deeper understanding of the dynamics of international policies that have an impact on digital sovereignty can be obtained. The data used in this study are secondary data, namely relevant international legal documents, such as the Budapest Agreement on Cybercrime and the General Data Protection Regulation (GDPR) of the European Union, as well as national policy documents and reports from relevant international organizations, such as the United Nations and the International Telecommunication Union (ITU).

The data collection technique used in this research is document analysis (Amanda et al., 2023). This technique involves identifying, evaluating and analyzing documents that relate to issues of digital sovereignty and international law. Each document was evaluated based on its relevance to the topic, the context in which it was discussed, and the time of publication, with more recent data being favored in order for the analysis to reflect the current state of affairs. The data obtained from the document analysis was then categorized based on key themes, such as cyber regulation, data privacy policy, and digital infrastructure protection. The collected data was analyzed using a thematic analysis approach. This process begins with coding, which is reading and understanding each document, then assigning codes to relevant parts of the data. After that, the codes were grouped into main themes and subthemes according to the research topic. Some of the main themes found included digital sovereignty, cybersecurity and data privacy, which were then further interpreted to answer the research questions regarding the impact of international law on digital sovereignty policies in the countries studied (Setiyawan et al., 2020; Thontowi, 2019).

To ensure the validity and reliability of the data, this study used data triangulation techniques, where data taken from different types of documents and sources were compared to find consistency or differences in the discussion of the same topic. This technique helped to ensure the accuracy of the research interpretations and findings. In addition, this study paid attention to research ethics by citing original sources appropriately and ensuring that all data came from trusted sources. Data interpretation is done objectively to avoid bias, especially in assessing each country's policy on digital sovereignty.

2. Materials and Methods

In this study, the approach used is a qualitative-descriptive approach with a multiple case study method to explore how international law plays a role in enforcing digital sovereignty in various countries (Setiyawan et al., 2020), (Berlianti et al., 2024). The case studies taken include digital policies and regulations in several countries, such as the European Union, the United States, and China, each of which has a different approach to managing sovereignty over digital resources. With this case study method, it is hoped that a deeper understanding can be obtained regarding the dynamics of international policies that have an impact on digital sovereignty. The data used in this study are secondary data, namely relevant international legal documents, such as the Budapest Agreement on Cybercrime and the General Data Protection Regulation (GDPR) of the European Union, as well as national policy documents and reports from related international organizations, such as the United Nations and the International Telecommunication Union (ITU).

The data collection technique used in this study is document analysis (Amanda et al., 2023). This technique involves identifying, evaluating, and analyzing documents related to digital sovereignty issues and international law. Each document is evaluated based on its relevance to the topic, the context discussed, and the time of publication, where more recent data is prioritized so that the analysis can describe the current conditions. The data obtained from the document analysis are then categorized based on the main themes, such as cyber regulation, data privacy policies, and digital infrastructure protection. The collected data are analyzed using a thematic analysis approach. This process begins with

coding, namely reading and understanding each document, then assigning codes to the relevant data sections. After that, the codes are grouped into main themes and subthemes according to the research topic. Some of the main themes found include digital sovereignty, cybersecurity, and data privacy, which are then further interpreted to answer research questions regarding the impact of international law on digital sovereignty policies in the countries studied (Setiyawan et al., 2020; Thontowi, 2019).

To ensure the validity and reliability of the data, this study uses data triangulation techniques, where data taken from various types of documents and sources are compared to find consistency or differences in the discussion of the same topic. This technique helps ensure the accuracy of the interpretation and findings of the study. In addition, this study pays attention to research ethics by citing original sources appropriately and ensuring that all data comes from trusted sources. Data interpretation is carried out objectively to avoid bias, especially in assessing the policies of each country regarding digital sovereignty.

3. Results and Discussion

3.1 An Analysis of Digital Sovereignty in Several Countries

The research found that countries' approaches to digital sovereignty are heavily influenced by their economic interests, national security, and political views on freedom of access to and control over digital information. The European Union, the United States and China exhibit diverse strategies in defending and protecting their sovereignty over digital resources.

a. Uni Eropa (UE)

The European Union is one of the most active entities in regulating the protection of its citizens' personal data through regulations such as the General Data Protection Regulation (GDPR). The GDPR is an important example of how supranational law plays a role in protecting citizens' data and giving individuals the right to control their personal data. Under the GDPR framework, foreign companies that collect and process data of EU citizens must comply with the regulation, even if they are located outside of EU jurisdiction. This shows that the EU is taking a protectionist as well as an inclusive approach, whereby any entity operating in the European market is subject to this policy. The EU's success in implementing GDPR reflects their efforts to strengthen digital sovereignty at the regional level, while inspiring other countries to adopt similar regulations to protect citizens' privacy rights and data security. In addition to the GDPR, the EU has also begun introducing regulations focused on artificial intelligence (Artificial Intelligence Act) that aim to ensure that AI technologies are used safely and in accordance with the human rights values prevailing in the region. While international law does not yet have a binding consensus on AI regulation, the EU's proactive steps show that the entity is seeking to steer international policy towards a more comprehensive and standardized regulation of digital resources.

b. Amerika Serikat (AS)

The United States' approach to digital sovereignty emphasizes internet freedom and technological innovation. The US has a different approach compared to the EU, where government regulation of data and privacy is generally less stringent than in Europe. The US emphasizes market freedom and the role of the private sector in managing data, so data protection policies in this country are mostly determined by the private sector, although some data protection laws have been implemented at the state level, such as the California Consumer Privacy Act (CCPA). However, in recent years, national security issues have prompted the US to take stricter measures against foreign companies that are deemed to potentially threaten national security, especially in the context of information and communication technology. The cases of Huawei and TikTok, for example, show that the US is increasingly protective of foreign influence in its digital infrastructure, issuing restrictive policies for these companies. This indicates that the US is starting to prioritize

aspects of digital sovereignty in several strategic sectors, especially related to cybersecurity and protection against digital espionage.

c. Tiongkok

China takes a much more protective path in protecting its digital sovereignty. The Chinese government actively controls digital infrastructure and restricts access to information from abroad through a policy known as the "Great Firewall of China." China also has very strict national data policies, such as the Cybersecurity Law and Data Security Law, which require foreign companies operating in China to store data relating to Chinese citizens domestically and report data usage to the government. This approach not only reflects China's complete control over national data but also signals that the country views data as an integral part of its national sovereignty. In China's perspective, data is seen as a strategic asset that must be protected from foreign influence. China's move illustrates a protectionist and centralized approach to digital sovereignty that differs from Western countries, which often prioritize the principle of openness.

3.2 The Role of International Law in Digital Sovereignty

This research finds that international law currently lacks universally binding instruments in regulating and protecting state digital sovereignty. Existing instruments, such as the Budapest Agreement on Cybercrime, only cover certain aspects of cybercrime, but not broader issues such as data privacy or digital data ownership. The absence of comprehensive international legal instruments results in an imbalance in the regulation of digital sovereignty between countries. Countries with greater digi-tal power tend to have more influence in setting the rules, while smaller or developing countries often have to follow the standards set by developed countries. For example, U.S.-based multinational technology companies have access to global data that can be used for economic gain, which in turn increases inequality between countries in terms of access to digital resources. In addition, some international efforts, such as the UN framework for cybersecurity, are voluntary and non-binding. This shows that while there is a global awareness of the importance of regulating digital resources, there is no strong and binding agreement among member states.

3.3 Dynamics and Tensions in Digital Sovereignty Arrangements

The results also show that different approaches between countries in managing digital sovereignty create tensions and fragmentation in the digital world. This fragmentation, often called the "splinternet," has the potential to reduce global connectedness and restrict data flows between countries. In this context, international law faces major challenges in creating standards that are acceptable to all parties without infringing on national sovereignty. For example, the protectionist approach taken by China has caused tensions with Western countries, which prioritize the principles of openness and freedom of information. On the other hand, the European Union's move with GDPR has positioned data protection regulations as a global standard, forcing many other countries to adapt their regulations in order to do business in Europe. The US itself often maintains a liberal approach, but with certain protective measures directed at foreign entities deemed to jeopardize its national security.

3.4 Implications for the Development of International Law

The findings indicate that international law needs to evolve to accommodate changes in the digital age. Issues of digital sovereignty, cybersecurity and data privacy require a more comprehensive and binding legal framework that can be accepted by all countries. Without clear inter-national regulations, each country will continue to develop policies that suit its national interests, potentially increasing fragmentation in the digital world. Ultimately, this research suggests that inter-national legal approaches need to be more responsive to the new challenges posed by advances in digital technology. One option that could be considered is a multilateral treaty that regulates various aspects of dig-

ital sovereignty, where each country has the freedom to manage data in its territory while respecting rights and global connectedness. Such international initiatives can help reduce tensions between countries, while building trust and cooperation in managing digital resources in a fair and sustainable manner.

4. Conclusions

This research concludes that international law has a significant but limited influence on the enforcement of state sovereignty over digital resources. The different approaches taken by the European Union, the United States and China show different perspectives and priorities in protecting their digital interests. The EU tends to put privacy rights and individual data protection at the center of its policies, which is reflected in regulations such as GDPR, and strengthens digital sovereignty by requiring foreign companies to comply with standards set in its territory. The United States, on the other hand, emphasizes market freedom and technological innovation, but has also begun to take a protective stance in the face of threats to national security. China takes a highly protectionist and centralized approach, where control over data and digital infrastructure is highly monitored by the government in order to maintain national sovereignty and stability. The absence of binding and comprehensive international legal instruments governing digital sovereignty creates a loophole that allows major powers to establish their own standards, sometimes imposing their interests on others. The results of this study show that international law needs to evolve to accommodate increasingly complex digital dynamics, especially in the aspects of cyber security, data privacy, and access to digital technology. In the absence of clear global standards, there is a growing risk of digital fragmentation (splinternet), which could undermine global connectivity and widen inequality in access to information between countries. This conclusion points to the importance of international cooperation in creating a legal framework that can accommodate the needs of each country without compromising their digital sovereignty. Multilateral agreements that address various aspects of digital sovereignty, with the principles of equality and mutual respect, are an important step towards reducing tensions and building fair and sustainable global digital governance.

References

Abimanyu, A. A., Setia, B. B., & Soegiharto, D. B. (2024). Analisis Kriminologi Mengenai Peredaran Narkoba Terkait dalam Keimigrasian. *Jurnal Ilmiah Universitas Batanghari Jambi*, *24*(1), 157–165.

Adha, L. A. (2020). Digitalisasi industri dan pengaruhnya terhadap ketenagakerjaan dan hubungan kerja di Indonesia. *Jurnal Kompilasi Hukum*, *5*(2), 267–298.

Amanda, M. D., Metalin, A., Puspita, I., Imanda, F. A., Maulana, R., & Santoso, G. (2023). Jurnal Pendidikan Transformatif (JPT) Kontribusi Masyarakat dalam Perspektif Ketahanan Nasional Indonesia di Era Digital Jurnal Pendidikan Transformatif (JPT). *Jurnal Pendidikan …*, *02*(03), 45–63.

Berlianti, D. F., Abid, A. Al, & Ruby, A. C. (2024). Penerapan Prinsip Hukum Internasional Dalam Penegakan Hukum Terhadap Kejahatan Siber Dan Serangan Siber, *7*, 1861–1864.

Buwono, S. R., Abubakar, L., & Handayani, T. (2022). Kesiapan Perbankan Menuju Transformasi Digital Pasca Pandemi Covid-19 Melalui Financial Technology (Fintech). *Jurnal Poros Hukum Padjadjaran*, *3*(2), 228–241.

Daniel, Shandi Negara, R., & Triadi, I. (2023). Penegakan Hukum Terhadap Kapal Asing Yang Melakukan Illegal Fishing Di Wilayah Perairan Indonesia Dalam Perspektif Hukum Laut Nasional Dan Internasional. *Triwikrama: Jurnal Ilmu Sosial* , *01*(9), 100–119.

Gani, T. A. (2023). *Kedaulatan data digital untuk integritas bangsa*. Syiah Kuala University Press.

Hamdan Mustameer. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. *Jurnal Yustika: Media Hukum Dan Keadilan*, *25*(01), 40–53. https://doi.org/10.24123/yustika.v25i01.5090

Jihansyah, A. S. (n.d.). KEBIJAKAN KEAMANAN INGGRIS: STUDI NATIONAL SECURITY COUNCIL.

Jl, A., Raya, M., Timur, J., Struktur, T., & Pedesaan, S. (2022). Implikasi Kebijakan Hukum Terhadap Struktur Sosial dalam Penguatan Kedaulatan Negara Arief Fahmi Lubis terhadap struktur sosial masyarakat desa di wilayah pedesaan Indonesia . Fokus utama perubahan signifikan dalam lanskap politik lokal . Otonomi desa , yang diperkuat melalui UU, *19*(2).

Kristianto, D. H. (2022). Tinjauan Yuridis Tindakan Eksploitasi Sumber Daya Perikanan Di Zona Ekonomi Eksklusif Indonesia Menurut Hukum Internasional. *Lex Privatum*, *10*(2), 1–12.

Muslich, M. (2022). *Pendidikan karakter: menjawab tantangan krisis multidimensional*. Bumi Aksara.

Nabila, A. P., Manabung, N. A., & Ramadhansha, A. C. (2024). Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional. *Indonesian Journal of Law*, *1*(1), 26–37.

Purwantoro, S. A. (2023). *Sistem Pertahanan Rakyat Semesta Menyongsong Indonesia Emas 2045*. Indonesia Emas Group.

Ramayanti, H., & Lubis, A. F. (2023). Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional. *Jurnal Hukum Dan HAM Wara Sains*, *2*(09), 904–912. https://doi.org/10.58812/jhhws.v2i09.672

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. *Perspektif*, *21*(3), 168. https://doi.org/10.30742/perspektif.v21i3.587

Setiyawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). Information Technology Regulatory Efforts in Dealing With Cyber Attack To Preserve State Sovereignty of the Republic of Indonesia. *Urnal USM Law*, *3*(2), 275–295.

Syafi'i, M. H., Supriyadi, A. A., Prihanto, Y., & Gultom, R. A. G. (2023). Kajian Ilmu Pertahanan dalam Strategi Pertahanan Negara Guna Menghadapi Ancaman Teknologi Digital di Indonesia. *Journal on Education*, *5*(2), 4063–4076. https://doi.org/10.31004/joe.v5i2.1100

Thontowi, J. (2019). Proxy War, Kejahatan Lintas Negara dan Pengaruhnya Terhadap Ketahanan Nasional Perspektif Hukum International. *Prosiding Senas POLHI Ke-2 Tahun 2019*, 202–223.

Trio Andi. (2023). Kedaulatan Di Bidang Informasi Dalam Era Digital: Tinjauan Teori Dan Hukum Internasional. *Judge : Jurnal Hukum*, *4*(01), 35–43. https://doi.org/10.54209/judge.v4i01.375

Wibawa, I. (2016). Era Digital (Pergeseran Paradigma Dari Hukum Modern Ke Post Modernisme). *Masalah-Masalah Hukum*, *45*(4), 285. https://doi.org/10.14710/mmh.45.4.2016.285-291

Yuniarti, S., & Herawati, E. (2020). Analisis Hukum Kedaulatan Digital Indonesia. *Pandecta*, *15*(2), 154–166.