RJOAS: Russian Journal of Agricultural and Socio-Economic Sciences
ISSN 2226-1184 (Online) | Issue 7(139), July 2023

UDC 304; DOI 10.18551/rjoas.2023-07.01

CYBERSTATE: AN ALTERNATIVE TO BUILDING LEGAL UNIFICATION BRINGING ABOUT LEGAL ORDER IN CYBERSOCIETY

Kusumaputra A., **Sudarsono**, **Fadli M.**, **Sukarmi**
Doctoral Program, Faculty of Law, University of Brawijaya, Malang, Indonesia
*E-mail: ardhiputra82@gmail.com

ABSTRACT
The world has been growing massively, giving rise to the presence of frequently used cyberspace in society. However, its presence triggers transnational criminal problems, which calls for a new legal order capable of serving as a solution to cybersociety-related problems. Departing from this overview, this research aims to investigate whether legal unification can serve as an alternative to building a legal order in cybersociety and how the idea of legal unification can come together with the existence of cyberspace to guarantee law-abiding cybersociety. This research focuses more on analyzing and finding new insight into law in the era of digitalization. In terms of normative law, legal unification is capable of setting a rationale to build cybersociety, but this measure requires transboundary cooperation to result in an international convention.

KEY WORDS
Cyberstate, legal unification, legal order, cybersociety.

A massive global shift has triggered the emergence of innovation in digital technology. Industrial Revolution 3.0 involving computers and automatization within the purview of a digital revolution began in the 1980s, marking the beginning of the Internet (digital technology) (Wijaya, 2019). The existence of the industrial era 4.0 proves it where digital technology is used more through Internet networks easing human life, the economy, and the government. The 4.0 industrial era — the cyber-physical system era — is more intended to strengthen the existence of electronic information. The inseparable way of life of human beings from the Internet is often linked to the phenomenon of the Internet of Things (IoT) (Hendarsyah, 2019).

Entering 2021, the situation of global civilization started to shift to the 5.0 Industry, where people started to balance their life with economic advancement, and the settlement of social issues started to combine physical aspects with the cyber world. Japan is known to have initiated the 5.0 society (Hendarsyah, 2019). Mayumi Fukuyama (M. Fukuyama, 2018) also elaborated that the 5.0 society design is intended to navigate human life into a more integrated pattern within a network of big data, virtual reality, cloud, artificial intelligence, or mixed reality. Principally, the existence of the 5.0 Society represents the development of the 4.0 industrial era, giving rise to a new habitat in a digital world to simplify human life.

From a legal perspective, especially in terms of the law applying in a state, there has been a considerable challenge. The law was shaped by a state through its governments, and the law must be capable of adjusting to the present conditions of the era of digital technology. The fact that the law is rigid is inevitable, and this nature is maintained to regulate the presence of digital technology. In other words, the law concerned is deemed weak simply because it is not malleable to the changing conditions.

From a different perspective, as a sovereign and territorial state, the state has its right to adhere to its sovereignty as a protection from any cyber threats. Thus, the state makes a set of regulations intended to restrict society, especially users to guarantee the security of the state. However, inevitably, a regulation cannot reach a criminal because he/she does not reside within Indonesia. Furthermore, if the state where a criminal is domiciled refers to different legal systems and extradition is almost impossible to perform, it is difficult to arrest and judge the criminal.

The emergence of digital technology gives birth to cyberspace, and this cannot be immediately claimed as part of the sovereignty of the state (Von Heinegg, 2012). Cyberspace guarantees the freedom of expression and communication. Users believe that cybercrime will require a more complex criminalization, as expressed by William Gibson (Makarim, 2004). In line with the development, although a state does not claim cyberspace, it can impose punishment on users proven to have violated the law as long as the users are within the jurisdiction of the law concerned.

This condition is seen from the legal perspective, triggering a new problematic condition. Philosophically, the principle of a state serves as the highest organization authorized to form a law, but it is getting weaker when a transboundary threat takes place. The law principally intended to regulate a situation for the sake of social order may not work properly when it does not have access to a virtual world, juridically sparking inefficacy of law. Although the regulation governing the presence of digital technology exists (specifically Law Number 11 of 2008 concerning Electronic Information and Transactions in Indonesia), it does not have the capacity to reach this point, leading to legal uncertainty.

Thus, it is essential to conduct a comprehensive study to help shape a supportive condition of a legal order, especially regarding the era of the 5.0 Society, as in line with national law, and international law, leading to legal unification (Yiannopoulos, 1961). Moreover, it is also important to refer to the theory of the law of convergence and the concept of cyber law as an instrument of analysis in building a comprehensive legal argument. With legal hermeneutics, the analysis is expected to be holistic in terms of textual and contextual scopes. To highlight, this research aims to answer the following issues: can legal unification serve as an alternative to building a legal order in cybersociety and how can the idea of this legal unification come together with the existence of cyberspace capable of creating a cyberstate in line with law-abiding cybersociety?

METHODS OF RESEARCH

This is normative (normative-juridical) research requiring library research to give information on legal aspects. This research refers to legal hermeneutics, theoretical, and conceptual approaches. The theory of the law of convergence and the concept of cyber law were also used, but other legal theories and concepts may also be used as long as they are relevant to the analysis of the legal issues concerned.

RESULTS AND DISCUSSION

The world is getting more modern as it is inseparable from the work of practitioners who build technology. Technology eases human life with the use of the Internet in a digital era. Imagination envisioning a new and human-made world capable of giving people the freedom of expression and allowing them to meet without being restricted in both time and space has been brought to life where the presence of digitalization is getting more obvious; this is known as cyberspace.

Seen from the perspective of the science of information technology, the presence of cyberspace is a manifestation of discrete data. With mathematical calculation (algorithm) coding is performed to give a real visualization (Bryant, 2001). Cyberspace saves varied encrypted electronic information. There is no exact restriction in cyberspace, and cyberspace serves as an infinity room as long as humans can grow their knowledge.

The uniqueness of cyberspace allows information technology freaks to deeply explore new things. Online games such as Minecraft, social media, virtual reality, mixed reality, or cryptocurrency (including controversial bitcoins) are some of the myriads of examples of the results of exploration into the science of information technology. It is like giving birth to a multiverse derived from a fictitious story.

Behind this uniqueness and content arising from cyberspace, threats against users are lurking. The confidentiality of information, security, and the sustainability of data or electronic information stored inside can pose risks. Cybercrime is highly likely to take place, making

use of the weaknesses of a system for personal gain. Cases of cybercrime have commonly taken place in a state or at a transboundary level Marco Gercke, “Cybercrime Understanding Cybercrime :,” Understanding Cybercrime: Phenomena, Challenges and Legal Response, no. ITU (2012): 366.

Seen from the legal perspective, the existence of cyberspace requires independent regulation, considering that these days digital technology is growing massively, calling for a regulation that can accommodate all cyber activities. Law is generally abstract and restricted to time and space (Mertokusumo, 2010). The law made should be adjusted to the condition of a region and the needs of the people in society. The effectiveness of law following the development of cyberspace cannot immediately apply to the cyber scope. That is, the existing law cannot easily penetrate cyberspace as a legal basis. Some classifications seem to allow the law to serve as the basis for cyberspace:

- Beneficial value; this point focuses more on the relevance between law and the needs of the digital world;
- Legal certainty; this value focuses more on the need for agreement/consensus in establishing a law that results in unification.

From the aspect of sovereignty, the clash between cyberspace and the existence of the sovereignty of the state is inevitable (F. Fukuyama, 2005). Many countries have been trying to claim cyberspace. This intention departed from the growing incidences of cybercrime taking place at a transboundary level, encouraging states to secure their own cyberspace by putting sovereignty therein.

However, cyberspace is unrestricted, and the claims made to position the interest of sovereignty in cyberspace can spark problems, especially when a regulation concerning cyberspace is inseparable from the interest of the state, considering that cyberspace represents a free space everyone could explore (Deguchi A.C Hirai, H Matsuoka, T. Nakano, K Oshima, M. Tai, 2020).

Philosophically, the basic objective of regulation is to set a legal order in society (Sieber, 2019). Law-making is addressed to the people in general, meaning that without society as the object governed by the law, the law concerned is not more than written artifacts. When the law fails to make people abide by it, the law will be nothing more than a symbol.

Law and people should go in a parallel direction. The governments with their power exist as law enforcers, while the law itself is also made by people. Law, people, culture, and authorities influence each other, and this is in line with the idea of Lynn Matter (Levett & Thompson, 2015) stating “law is not autonomous, standing outside of the social world, but is deeply embedded within society. While political scientists recognize the fundamentally political nature of law, the law and society perspective take this assumption several steps further by pointing to ways in which law is socially and historically constructed, how law both reflects and impacts culture and how inequalities are reinforced through differential access to, and competence with legal procedures and institutions”.

In a modern world like today, there has been an immediate shift, demanding a more dynamic regulation. In other words, the law is not merely made to put people in order, but it is also intended to accommodate the present conditions in society as long as it does not contravene the general norms. Especially today, cybesociety is also linked with metaverse development (L. Rosenberg, 2022). They are internet users actively utilizing the internet for every need. Some have even transferred their real life to cyberspace (L. Rosenberg, 2022).

However, cyberspace is prone to problems, ranging from data theft, hacking, cyber bullying to money laundering. Laws applied in most countries tend to restrict or not to be incongruous with the real conditions of the enforcement. As a result, several cases like expressing views are often taken as part of hate speech. This condition is considered inappropriate.

In such a condition, legal measures need to be taken to lead to legal certainty in assuring security. The thought of legal unification raises from the basis implying that legal unification represents an adjustment to a standard or the provision of law. The unification process requires several steps such as observation, discussion, planning, analysis,

formation, and signing. The idea of this legal unification was also adopted from international law that is transnational. George A. Zaphiriou (Zaphiriou, 1994) stated “It direct change of rules, standard, or processes in order to avoid conflicts and bring about equivalence”. The primary objective of unification is to assure order to avert any likelihood of conflict of legal norms, especially transnational ones.

Therefore, the process of this legal unification in terms of setting the legal order in cybersociety, needs to involve several states voluntarily shaping the unity of the new law to be further implemented in the cyber world, thereby forming the international convention within the scope of cyberspace (L. B. Rosenberg, 2022).

Seen from a sociological perspective, conducting legal unification that is transnational is not an easy matter, but it is not something impossible as well. In terms of international trade, this era is heading 5.0 industrial era, and there have been massive changes taking place in no time.

The existence of cyberspace has indeed been dominated by superpower states such as China (Creemers, 2021). Platforms are available to save data, and Indonesia as a developing country needs support like other developing countries in Southeast Asia.

The image of unification in cyberspace seems to be in line with the objective to unite the world, considering that every person communicates across countries using cyberspace which also poses risks that have to be controlled by law (Tsagourias & Buchan, 2015).

Google has dominated data services in cyberspace, but Google is not a state. Seen from the perspective of sovereignty, it is prone to violation. A platform like this always starts with a standard agreement and it gives no freedom of choice for users using Google service. In other words, in terms of the responsibility aspect, Google relies on the state that made it. This condition implies that branch offices and partnerships between the platform and states are required.

It is, however, important to know that this massive developed world calls for standard regulatory structures. Modernization has encouraged the breakthrough of accommodating the need for digitalization to take place, thereby making the state capable of fulfilling the needs of its people.

Cyberspace cannot be principally claimed by any state unless it refers to the will of the users or IP address used. According to the theory of cyber law, cyberspace serves as a medium of global communication based on the freedom of information and communication (free flow of information). This new nature seems to give the freedom of expression, but still, this freedom has its limit, as expressed by Yiannapoulos (Anonymous, 2018) responding that “Twitter doesn’t stand for free speech. What they do stand for is a carefully crafted façade of leftist-approved ideas and conservatives that don’t stray too far from safe (globalist) ideas. Like so many platforms before them, their efforts to enforce groupthink will be their undoing.” Twitter later stated that the company was taking steps to improve its ability to act against abusive behavior.

Internet users are connected to cyberspace and bound to their state, meaning that they must abide by the law of the state. In Indonesia, the existence of cyberspace is bound to the regulatory provisions outlined in Law concerning Electronic Information and Transactions. However, these provisions, according to the nationality principle, are binding due to citizenship status and the domicile within Indonesia. Different rules and regulations in other countries will certainly present another problem in law enforcement.

Hacking elaborated as “gaining unauthorized access to a computer system and, as such, is conceptually analogous to real word trespassing” is one of the cases. This is considered illegal, once committed by an Indonesian in Australia, where he hacked a site owned by a person residing in China. According to Law concerning Electronic Information and Transactions in Indonesia, the hacker is punishable under Article 37 of the law concerned, but it will present another problem when it comes to the provisions that apply in China or Australia. For example, Australia may expect the hacker to be judged under the law of the state where the crime took place. This situation leads to a quandary of law enforcement notwithstanding the possibility of extradition to take place.

Compared to the law of the European Union, the convergence of law and information technology has frequently taken place within the scope of the European Union, which asserts that legal unification is more possible to do. The Eighth UN Congress on the Prevention of Crime and Treatment of Offenders, Havana, Cuba, in 1990 is the first milestone of cybercrime prevention. The Group of Eight (G8) 1997 consists of Canada, Germany, France, Italy, Japan, England, the USA, and Russia. The G8's primary task is to improve the capacity of inquiries into and charges against high-tech crime and to reinforce the regime of international law for extradition and reciprocal aid to ensure that there is no safe place for cyber offenders in the world. The existence of G8 is dominated by superpower countries. Apart from the particular political interest behind which this group was formed, the power to initiate legal unification seems obvious.

However, it is inevitable that the binding force of an international convention only applies to those involved as members and doing ratification. The measures taken to go to legal unification are intended to set uniformity of the standards for states, legal actions, and resolutions, highlighting the obedience to the convention as agreed upon. Some conventions such as European Convention on Cyber Crime in European Union are still applied at a regional level but this convention is open to other countries outside European Union, requiring other countries to abide by the provisions regulated therein.

General Data Protection Regulation (GDPR) having been applied in European Union since 14 April 2016 has initiated a breakthrough in law. This regulation protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of their personal data (Bowman & Gufflet, 2017). Although it is binding only to the states in European Union, its existence affects the law in Indonesia, encouraging this state to make Law Number 27 of 2022 concerning Data Protection. The effectuation of GDPR should be seen as an embryo marking the beginning of the existence of a cyberstate structure. The assurance of the European Union to make legal norms affect other states and it should be taken as a "golden moment" in structuring cybersociety at a global level. This is also aimed to reduce the likelihood of acquisition of control by giant private companies and return the crucial role of the state (Spalević & Vićentijević, 2022).

In an effort to build a transnational legal unification and take legal acts with legal certainty, it is essential to highlight the unification of regulations to allow for the establishment of the structure of cyberstate and impose consequences on criminal offenses in cyberspace and transnational offenders, place countries in the position authorized in the enforcement, and make a breakthrough that paves the way to the 5.0 industrial era by strengthening the existence of cyberstate with legal provisions agreed upon by all states worldwide.

CONCLUSION

Legal unification is capable of initiating a breakthrough as a basis for bringing about legal order in cybersociety and restructuring conventional thoughts and the law in a digital era. Legal unification is essential to help maximize the role of the states to initiate a breakthrough to build cyberstate, giving rise to more harmonious norms of transnational digitalization.

REFERENCES

1. Anonymous. (2018). An Introduction to Law and Society. SAGE Publication Inc.
2. Bowman, J., & Gufflet, M. (2017). Practitioner's Corner Meeting the Challenge of a Global GDPR and BCR Programme. European Data Protection Law Review, 3(2), 257–261.
3. Bryant, R. (2001). What Kind of Space is Cyberspace? Minerva - An Internet Journal of Philosophy, 5, 138–155.
4. Creemers, R. (2021). China's Cyber Governance Institutions.
5. Deguchi A.C Hirai, H Matsuoka, T. Nakano, K Oshima, M. Tai, and S. T. (2020). Society 5.0 A People-Centric Super-Smart Society, Spinger Open 2020. The University of Tokyo.

6. Fukuyama, F. (2005). State Building: Governance and World Order in the 21st Century, (Terjemahan A. Zaim Rofiqi). Gramedia.
7. Fukuyama, M. (2018). Society 5.0: Aiming for a New Human-centered Society. Japan Spotlight, 27(August), 47–50.
8. Gercke, M. (2012). Cybercrime Understanding Cybercrime : Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU, 366. https://doi.org/10.1088/1367-2630/11/1/013005
9. Hendarsyah, D. (2019). E-Commerce Di Era Industri 4.0 and Society 5.0. Iqtishaduna: Jurnal Ilmiah Ekonomi Kita, 8(2), 171–184. https://doi.org/10.46367/iqtishaduna.v8i2.170
10. Levett, L. M., & Thompson, A. M. (2015). Law and Society. International Encyclopedia of the Social & Behavioral Sciences: Second Edition, November, 509–514. https://doi.org/10.1016/B978-0-08-097086-8.45065-8
11. Makarim, E. (2004). Kompilasi Hukum Telematika. Rajawali Pers.
12. Mertokusumo, S. (2010). Mengenal Hukum Suatu Pengantar. Universitas Atma Jaya Yogyakarta.
13. Rosenberg, L. (2022). Regulation of the Metaverse: A Roadmap The risks and regulatory solutions for largescale consumer platforms. ACM International Conference Proceeding Series, July, 21–26. https://doi.org/10.1145/3546607.3546611
14. Rosenberg, L. B. (2022). Regulating the Metaverse, a Blueprint for the Future. XR Salento, July, 263–272. https://doi.org/10.1007/978-3-031-15546-8_23
15. Sieber, U. (2019). Legal Order in a Global World – The Development of a Fragmented System of National, International, and Private Norms –. Max Planck Yearbook of United Nations Law Online, 14(1), 1–49. https://doi.org/10.1163/18757413-90000048
16. Spalević, Ž., & Vićentijević, K. (2022). GDPR and challenges of personal data protection. The European Journal of Applied Economics, 19(1), 55–65.
17. Tsagourias, N., & Buchan, R. (2015). Research Handbook on International Law and Cyberspace. Edward Elgar Publishing Limited.
18. Von Heinegg, W. H. (2012). Legal implications of territorial sovereignty in cyberspace. 2012 4th International Conference on Cyber Conflict, CYCON 2012 - Proceedings, 7–19.
19. Wijaya, W. V. (2019). Sejarah and Evolusi Era Digital.
20. Yiannopoulos, A. N. (1961). Conflict of Laws and Unification of Law by International Convention : The Experience of the Brussels Convention of 1924. Louisiana Law Review, 21(3).
21. Zaphiriou, G. A. (1994). Unification and Harmonization of Law Relating to Global and Regional Trading. Nothern Illinois University Law Review, 14, 407–419.