sciendo

Critical views on the phenomenon of EU digital sovereignty through the prism of global data governance reality: main obstacles and challenges

Lusine Vardanyan
&
Hovsep Kocharyan*

Summary: This article is devoted to determining the role and place of the EU in the international information space, as well as identifying problematic aspects and existing challenges that the EU faces in implementing its digital strategy in the field of data governance and protection. In the context of the growing influence of such key political figures as, for example, the USA and China, which have dominant influence on the digital economy, the issue of proper ensuring the digital sovereignty of the EU in the field of global data governance comes to the fore. This is due to the fact that it is the digital sovereignty that should guarantee the strategic autonomy of the EU in the digital world in the context of the EU's increasing dependence on foreign technologies and services and a shortage of investments in the digital sector. In this research, the authors focus on the need to develop and use a model of multilateral participation in the field of data governance and protection in the digital world, which, in turn, implies prevention of weakening the role of the state in regulating the digital market, since it is the states (including the EU) that are the primary guarantors of human rights protection in the digital world.

Keywords: digital sovereignty, data protection, digitalization, EU, digital strategy.

Citation: VARDANYAN, L.; KOCHARYAN, H. Critical views on the phenomenon of EU digital sovereignty through the prism of global data governance reality: main obstacles and challenges. *European Studies – the*

* Lusine Vardanyan is a PhD student at the Department of International and European Law, Faculty of Law, Palacký University Olomouc, Czech Republic, e-mail: lucyrossetti77@gmail.com; Hovsep Kocharyan is a PhD student at the Department of International and European Law, Faculty of Law, Palacký University Olomouc, Czech Republic, e-mail: hovsep.kocharyan01@upol.cz

Review of European law, Economics and Politics, 2022, vol. 9, no. 2, pp. 110–132 DOI: 10.2478/eustu-2022-0016.

Ackowledgements: This article has been written on behalf of the grant project Reg. no. CZ.02.2.69/0.0/0.0/19_073/0016713 „The Role of the EU in the Quest for Digital Sovereignty" (DSGC-2021-0198).

1. Introduction

The issue of digital sovereignty of the EU is still one of the controversial and debatable issues facing EU law, which has become relevant in the context of growing digitalization in many spheres of public life, where outdated and traditional communication means are being actively replaced by new, digital ones.[1] The dependence on digital technologies became even more noticeable during the Covid-19 pandemic, which further strengthened the EU's conviction of the need to quickly achieve strategic autonomy in the development of its own digital solutions.[2] As J. Pohle and T. Thiel correctly point out: „The concept of digital sovereignty has become a powerful term in political discourse that seeks to reinstate the nation state, including the national economy and the nation's citizens, as a relevant category in the global governance of digital infrastructures and the development of digital technologies. We can expect the concept of digital sovereignty to continue to gain even more political currency in the years to come, given the broad deployment of highly invasive digital technologies ranging from artificial intelligence to the „Internet of Things".[3]

At the same time, the EU's growing interest in achieving strategic autonomy in the digital world is not only fully consistent with its fundamental principles and values enshrined in the EU primary law,[4] but also with its ambitions to strengthen its position in the digital economy. Such ambitions are not unfounded: nowadays the EU acts as one of the most developed economic integrations in the world, and in the conditions of rapid digitalization of many spheres of life, it becomes

[1] COUTURE, S., TOUPIN, S. What does the notion of „sovereignty" mean when referring to the digital? *New Media & Society*. 2019, vol. 21, no. 10, pp. 2305–2322 [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107272

[2] AKTOUDIANAKIS, A. Fostering Europe's Strategic Autonomy: Digital sovereignty for growth, rules and cooperation. In: Konrad Adenauer Stiftung. European Policy Centre. 2020, pp. 1–24 [online]. Available at: https://www.epc.eu/content/PDF/2020/Digital_SA_paper_EPC_and_KAS.pdf

[3] POHLE, J., THIEL, T. Digital sovereignty. *Internet Policy Review*. 2020, vol. 9, no. 4, pp. 1–19.

[4] For example, according to Art. 2 of TEU, one of such EU values is respect for human rights (in the digital world), including the rights to personal data protection enshrined in the CFR (2000).

clear that the EU simply cannot afford to weaken its position, since the weakening of the EU will mean the „decline" of European integration in the conditions of worsening digitalization. The seriousness of this issue is also understood by European politicians. That is why the cornerstones of the EU policy in achieving strategic autonomy in the digital world are such legal instruments for data protection as GDPR[5], DGA[6], AIA[7] and so on, which, in turn, has its own rational explanation. The fact is that nowadays human data is becoming the driving force and the „new currency" of digital relations,[8] and their governance and protection becomes the key to strengthening the digital autonomy of the EU. However, in this context, the following questions come to the fore:

1. What are the main obstacles and challenges currently facing the EU in the process of implementing its digital data governance and protection policy?
2. What would be the most optimal way for the EU to strengthen its strategic autonomy in the digital world?

In this article, we focus our attention on the main challenges and obstacles that the EU faces in its practice when implementing its concept of digital sovereignty in the context of data protection, as well as will propose our vision for strengthening the EU's power in digital world.

2. The role and place of the EU in the context of existing global data governance realities

Before proceeding to a direct consideration of the main challenges and obstacles facing the EU in the digital world, it is necessary to understand, what place the EU occupies in the context of global data governance reality. Nowadays, in the conditions of ever-growing influence of BigTech companies on the digital space, the digital world more and more turns into an „arena of struggle", which has its logical explanation. The digital world provides new opportunities for the most

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (hereinafter – GDPR)

[6] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) (hereinafter – DGA)

[7] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (hereinafter – AIA)

[8] GATES, C., MATTHEWS, P. Data Is the New Currency. *New Security Paradigms Workshop*. 2014., pp.105–116.

developed competing world economies to take a dominant position in the digital economy, which in turn leads to a situation of Hobbesian *bellum omnium contra omnes* in the digital world.[9] In such circumstances, the EU refers to its concept of digital sovereignty to assert its claims regarding data and digital infrastructure in the context of strengthening the role of multinational BigTech companies in the EU economy, thereby seeking to restore independence from foreign digital service providers and increase its control over these strategic assets. To achieve this goal, the EU is trying to adapt the new relations of the digital world to the already existing categories of the traditional (Westphalian) understanding of sovereignty in order to maintain the defining role of the state in cyberspace, positioning itself as its main regulator not only unilaterally, but also within the framework of multilateral agreements.[10] This policy is fully justified: in the conditions of a „network society" and its „creative chaos", it is the states that should be responsible for regulating information flows.[11] Indeed, we should not forget that the EU, through the adoption of the EU Charter on Fundamental Rights (2000) (hereinafter – the „CFT"), thereby became the guarantor of the protection of these fundamental human rights, including the right to personal data protection in both „offline" and „online" worlds. The weakening of the EU's role in the digital world will lead to a situation where the EU will be unable to protect human rights online, including the right to data protection, and the role of such a guarantor will *de facto* be performed by the most powerful players of the digital economy, such as, for example, BigTech companies, which, of course, will always be guided by their economic interests and which, in its turn, will reduce to nullify the protection of human rights in the digital world. It is no coincidence that the President of France Emmanuel Macron stresses the need to strenthen the EU's sovereignty in the digital world as one of the fundamental steps to „refound" the EU.[12]

However, in terms of achieving strategic autonomy, not everything is going smoothly for the EU. In the conditions of growing fragmentation in the digital space it is becoming increasingly difficult to determine, what are the actual boundaries of the EU's sovereignty in the digital space, as well as what is the place and role of the EU in the digital space in the light of growing influence of various transnational BigTech companies in the processes taking place in the digital world.

---

[9] HOBBES, T. *Leviathan*. Hamburg: Meiner Verlag. Philosophische Bibliothek. 2005, pp. 610.

[10] THIEL, T. Unendliche Weiten ...? Umkämpfte Grenzen Im Internet. *INDES – Zeitschrift für Politik und Gesellschaft*. 2012, vol. 1, no. 4, pp. 61–67.

[11] WEBSTER, F. *Theories of the Information Society. Second Edition*. Moscow: Aspect Press. 2004, pp. 134–135.

[12] L'OBS, L. *Les 6 piliers du plan de Macron pour „refonder l'Europe"* [online]. Available at: https://www.nouvelobs.com/politique/20170926.OBS5171/les-6-piliers-du-plan-de-macron-pourrefonder-l-europe.html

Moreover, the concept of digital sovereignty itself is understood differently in various states (including the EU). For example, it is impossible to equate the digital sovereignty of the EU, China or the USA, because we are talking about different phenomena, even though we use the same term. We can even point out the significant differences between the conceptual approaches to data governance and protection policies that the EU and the USA adhere to. They have different legal systems in the field of personal data governance and protection, as they are based on two radically different concepts of privacy. For example, the EU, after the adoption of the GDPR, created a single (centralized) mechanism for the protection of personal data for its citizens, based on the right to privacy, formulated in the framework of the European Convention on Human Rights (1950) („ECHR") and the EU Charter on Fundamental Rights (2000) („CFT"), and subsequently developed by the case-law of the European Supranational Courts.

As for the USA, its legal system, unlike the EU, proceeds from the need to regulate the data governance and protection in certain areas of economy. In other words, in the USA, privacy is protected only in the context of commercial activity, where the data subject is considered not as a citizen, but as a consumer. This can even be seen by the example of what institutional mechanisms are used for data governance and protection in the EU and the USA. So, while in the EU the centralized national data protection authorities (DPA) are responsible for data protection, in the USA the Federal Trade Commission acts as the main data protection authority, i.e. an independent agency of the US government, which is designed to protect the rights and legitimate interests of consumers.[13] As I. Jolly correctly observes: „(…) in contrast to the European Union's data protection approach, which in many ways represents the gold standard of privacy protections, the dominant approach in the United States is grounded in consumer protection regulations (…) In stark contrast to the rights enjoyed by European consumers, American consumers do not possess „a right to be forgotten". Nor is there a single federal notification law that mandates notification in case of a data breach".[14] Indeed, the GDPR and mainly its right to be forgotten, developed by the CJEU's case-law, are trying to strengthen the EU's digital sovereignty through „putting individuals in control of their data" and turning the EU into „a standard-setter in privacy and data protection".[15]

[13] The Federal Trade Commission works to prevent fraudulent, deceptive, and unfair business practices. They also provide information to help consumers spot, stop, and avoid scams and fraud. Available at: https://www.usa.gov/federal-agencies/federal-trade-commission

[14] JOLLY, I. *Data Protection in the United States. Overview* [online]. Available at: https://content.next.westlaw.com/6-502-0467?transition

[15] MADIEGA, T. *Digital sovereignty for Europe* [online]. Available at: https://policycommons.net/artifacts/1336893/digital-sovereignty-for-europe/1944437/ on 04 Sep 2022. CID: 20.500.12592/5n1gmm

At the same time, the EU itself also positions its digital sovereignty as different from the approach of other digital leaders, such as the USA and China. However, being an integrational supranational *sui generis* organization,[16] the EU has its own, peculiar only to it, issues of implementing its strategic autonomy through the prism of its digital sovereignty, which other digital leaders do not face.[17] In particular, in the context of the EU, the discussion about sovereignty is particularly difficult: when recognizing „digital sovereignty" as a derivative of „sovereignty" in relation to the EU, it translates the discussion into the area of the legal nature of the EU, the issue of the transfers of powers from the sovereign Member States to the EU, which does not follow from the EU primary law, especially when the term „sovereignty" is not used in them at all. In addition, it is possible that the goals of a single EU Member State in the field of digital sovereignty may not coincide with the goals of the EU as a whole, despite its membership in the EU. Consequently, the question arises on how should the digital sovereignty of the EU Member States and the EU itself relate to each other, and what should be the boundaries between them? Besides, as it is noted by H. Roberts, J. Cowl and others: „(...) the extent to which it is viable that choices could be made by the EU ‚independently' is unclear, and the identities of those actors with whom the EU is competing (i.e., those who might also claim digital sovereignty) are frequently unstated."[18]

In addition, with the dynamic development of legal relations, the essence and legal nature of the EU itself is also changing, and the EU is increasingly „absorbing" the sovereign rights of its Member States to achieve its goals.[19] For example, the EU (like its predecessors) was initially created as a political and economic project, but later, with the adoption of the EU Charter of Fundamental Human Rights, it also became a human rights organization (like the Council of Europe), which undoubtedly changed its legal status. Nowadays the digital world is becoming one of the spaces of vital interest to the EU, where the EU is trying

[16] PEROČEVIĆ, K. European Union Legal Nature: EU As Sui Generis – A Platypus-Like Society. *Inter EU Law East*. 2017, vol. 4, no. 2, pp. 101–116.

[17] HAMUĽÁK, O. „Lessons from the Constitutional Mythology" or How to Reconcile the Concept of State Sovereignty with European Integration. *DANUBE: Law and Economics Review.* 2015, vol. 6, no. 2, pp. 75–90.

[18] ROBERTS, H., COWL, J., CASONARI, F., MORLEY, J., TADDEO, M., FLORIDI, M. Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies. *Internet Policy Review*, 2021, Forthcoming, pp. 1–26. [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3937345

[19] DI STASI. A. The Enlargement of Competences of the European Union between State Sovereignty and the so-called European Sovereignty: Focus on the Limits of Applicability of the Charter of Fundamental Rights of the European Union. *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*. 2020, vol. 22, no. 45, pp. 131–154.

to establish its dominance. Consequently, the problem of the legal nature of the EU remains even more relevant in the context of the EU's ambitions to implement its digital policy, which may also cause concerns among the EU Member States themselves in terms of the risk of federalization and disproportionate loss of their sovereign rights. Although in our opinion, even the very expression „digital sovereignty of the EU" used in various EU documents already shows the intentions of such federalization on the part of the EU, which in the future may cause conflicts between the EU and its Member States.

As we can see, on the way to implementing its strategic autonomy in the digital world, the EU has to face the interests of different subjects of the digital economy at various (both internal and external) levels, having different goals and priorities of digital policy. At the same time, despite the obvious importance of gaining digital sovereignty, the EU has not yet managed to develop a unified approach to understanding what political and diplomatic measures it is ready to take in order to achieve its strategic autonomy in the digital world. The EU only positions itself as a regulatory „superpower", and Ursula von der Leyen stresses that the EU will „jointly define standards for this new generation of technologies that will become the global norm".[20] This is also facilitated by the judicial practice of the CJEU, which makes extraterritorial decisions on disputes related to data protection in the digital world. For example, in the case of *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, the Court has expanded the possibility of applying the right to be forgotten outside the EU territory in the cases of defamation.[21] However, in such cases, the problem arises of ensuring that the CJEU applies its judgments outside its territory. Although by its judgment, the Court made it clear that data protection is „floor, not a ceiling",[22] which can be traced by the example of the smooth evolution of the judicial practice of the CJEU on the right to be forgotten, but by what legal means is it able to ensure the extraterritoriality of its decisions in reality? Maybe such a judgment can be considered as an advantage, but we adhere to the position that it is a disadvantage if we take into account that the judgment of the CJEU, which tries to extend the EU data protection laws to the global digital order, will not have „coercive force". This means that making decisions devoid of „coercive force" can significantly reduce the credibility of the CJEU

[20] See: EDRi: *Von der Leyen: An ambitious agenda for digital rights* [online]. Available at: https://edri.org/our-work/von-der-leyen-ambitious-agenda-for-digital-rights/

[21] See: Case C-18/18. *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, Judgment of the Court (Third Chamber) of 3 October 2019.

[22] SAMONTE, M. *Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law* [online]. Available at: https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/

itself.[23] Moreover, the (in)ability of such enforcement faces a number of difficulties in the digital world, that combines non-physical aspects of cyberspace with extraterritoriality. As it is emphasized by J. Goldsmith and T. Wu: „(w)ith few exceptions governments can use their coercive powers only within their borders and control offshore Internet communications only by controlling local intermediaries, local assets, and local persons".[24] Besides, the more limited the connection with the foreign jurisdiction, the more likely it is that the foreign jurisdiction will not enforce the judgment.

It should be noted that such a situation, when the EU is trying to extend its data protection jurisdiction beyond its geographical territories, can have serious consequences for the EU, since the digital policy of Europeans on the way to digital sovereignty and its achievement can be perceived in completely different ways by the EU's digital partners. In particular, in the field of Internet governance, Chinese government seeks to fully control the entire digital infrastructure and information on its territory through a content filtering system known as „The Great Firewall of China".[25] As S. Wood, S. Hoffman and others point out: „Through wide-ranging content-filtering and censorship (dubbed ‚the Great Firewall') it has created, in effect, a separate internet ecosystem. Far-reaching data localisation requirements, restrictions on encryption, deep packet inspection, and indigenous technology requirements give Chinese authorities unparalleled control of the national cyberspace'."[26] In such circumstances, the EU's digital sovereignty may be perceived, for example, by the Chinese authorities in a negative way and cause strained relations between these digital powers in the digital world.

It is worth noting that at the current stage, the EU is still able to achieve certain results in the process of implementing its strategic autonomy in the digital world, taking into account the political and legal resources available to it. In particular, many foreign companies, including BigTech companies located outside the EU, develop their privacy policies in strict accordance with the requirements of the GDPR and other EU data protection tools, which suggests that EU law is becoming a kind of benchmark for data protection on a global scale in the prevailing „digital chaos". Most likely, this is facilitated by the fear of

[23] KOCHARYAN, H., VARDANYAN, L., HAMUĽÁK, O., KERIKMÄE, T. Critical Views on the Right to Be Forgotten After the Entry Into Force of the GDPR: Is it Able to Effectively Ensure Our Privacy? *International and Comparative Law Review*. 2021, vol. 21, no. 2, pp. 96–115.

[24] GOLDSMITH, J., WU, T. (ed.). *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press, 2006, pp. 238.

[25] SCHIA,-N.,-GJESVIK,-L. China's-cyber-sovereignty. *NUPI: Policy Brief*. 2017, vol. 2, pp. 1–4.

[26] WOOD, S, HOFFMANN, S., MCFADDEN, M., KAUR, A., WONGSAROJ, S., SCHOENTGEN, A., FORSYTH, G., WILKINSON, L. *Digital Sovereignty: the overlap and conflict between states, enterprises and citizens* [online]. Available at: https://oxil.uk/publications/2021-01-20-plum-digital-sovereignty/

being subjected to huge monetary sanctions provided for breaching the GDPR requirements, which keeps even large-scale BigTech companies located outside the EU under constant pressure, not to mention the European companies themselves. Nevertheless, despite some success, the EU should take a far-sighted look at this situation: the EU's digital jurisdiction still remains fragile and vulnerable. This means that if the EU does not think about new practical solutions to strengthen its strategic autonomy in the digital world through its concept of digital sovereignty in the long term, sooner or later such EU policy will fail in the digital race. What problems the EU has to solve in order to strengthen its strategic autonomy in the digital world, we will describe in more detail in the following sections of this article.

3. The EU's digital sovereignty as a simple digitalization of Westphalian sovereignty in the field of data governance?

First of all, the very understanding of the concept of digital sovereignty of the EU itself is not without problems, which is ambiguous in the academic literature and causes a number of not only theoretical, but also practical discussions. As it is noted by R. Bellanova, H. Carrapico and D. Duez: „The very idea of an EU digital sovereignty is puzzling. On the one hand, it conflates digital and sovereignty – which are two terms that orthodox EU studies are not used to conflating. On the other hand, it also conflates EU and sovereignty, whose nexus has been a mainstay in academic and political debates on European integration."[27]

Although it can be stated that a number of scholars, considering the issue of digital sovereignty of the EU, depart from its understanding through the state-centric aspect or through the territorial dependence of the exercise of power in the digital space, which is not accidental.[28] The fact is that we are used to understanding sovereignty through the prism of Westphalian sovereignty, in which sovereignty is given a territorial character, which can be traced in the analysis

[27] BELLANOVA, R., CARRAPICO, H., DUEZ, D. Digital/sovereignty and European security integration: an introduction. *European Security*. 2022, vol. 31, no. 3, pp. 337–355.

[28] GÁBRIŠ, T., HAMUĽÁK, O. 5G and Digital Sovereignty of the EU: The Slovak Way. *TalTech Journal of European Studies*. 2021, vol. 11, no. 2, pp. 25–47; RUOHONEN, J. The Treachery of Images in the Digital Sovereignty Debate. *Minds & Machines*. 2021, vol. 31, pp.-439–456.; FISCHER, D. The digital sovereignty trick: why the sovereignty discourse fails to address the structural dependencies of digital capitalism in the global south. *Z Politikwiss.* 2022, vol. 32, pp. 383–402.

of various international treaties. For example, article 2 of the Draft Declaration of the Rights and Obligations of States (1949)[29] provides that each State has the right to exercise jurisdiction over its territory and over all persons and objects located within it, in compliance with the immunities recognized by international law, while article 2 of the UN Convention on the International Law of the Sea (1928)[30] provides that the sovereignty of a coastal State extends beyond its land territory and internal waters, and in the case of an archipelago State – its archipelagic waters, to the adjacent sea belt, called the territorial sea, to the airspace above the territorial sea, as well as to its bottom and subsoil. Another example is the Chicago Convention (1944),[31] article 1 of which provides that each State has full and exclusive sovereignty over the airspace over its territory.

Another important international instrument that shows the connection of sovereignty with territory is the Montevideo Convention on the Rights and Obligations of States (1933).[32] Thus, according to article 1 of this Convention, the „State" as a subject of international law must have the following qualities: *(1) permanent population*; *(2) defined territory*; *(3) government*; and *(4) ability to enter into relations with other states*. It can be said that this definition in Article 1 of the Montevideo Convention has acquired the status of international customary law, and since its adoption it has been repeatedly confirmed in international judicial practice.[33] In particular, the Arbitration Commission of the European Conference on Yugoslavia expressed the opinion that *„the State is commonly defined as a community which consists of a territory and a population subject to an organized political authority; that such a state is characterized by sovereignty"*.[34]

In addition, in the case of *Island of Palmas case (Netherlands v.USA)* (1928) the PCIJ held that: *„...(t)he development of the national organisation of States during the last few centuries and, as a corollary, the development of international law, have established* ***this principle of the exclusive competence of the State in regard to its own territory*** *(...)"*,[35] while in the case of *Barce-*

[29] Draft declaration on rights and duties of states. General Assembly resolution 375 (IV) of 6 December 1949

[30] United Nations Convention on the Law of the Sea of 10 December 1982

[31] Convention on International Civil Aviation, signed at Chicago, on 7 December 1944 (Chicago Convention)

[32] Convention on Rights and Duties of States Signed at Montevideo on December 26, 1933 (Montevideo Convention)

[33] LAUTERPACHT, H. *Recognition in International Law*. Cambridge: Cambridge University Press, 2012, pp. 419.

[34] Opinion No. 1 of the Arbitration Commission of the European Conference in Yugoslavia. See in: SHAW, M. N. *International Law*. Cambridge: Cambridge University Press, 2008, pp. 198.

[35] See: *Island of Palmas (Netherlands v. USA)*. Judgment. Permanent Court of International Justice. 4 April 1928.

lona Traction (1970) (Belgium v. Spain)[36] the ICJ emphasized that, state sovereignty and the principles of non-interference require restrictions imposed by international law on the exercise of jurisdiction in cases with foreign elements. As one can see, sovereignty is directly dependent on a certain territory, which is a natural condition for the existing and functioning of the state.[37] At the same time, the requirement of a certain territory in article 1 of the Montevideo Convention refers to borders, and a certain territory means a certain geographical space, different from other geographical spaces, over which the State exercises its exclusive power.

However, how to define such an EU territory in cyberspace, and how to ensure the functioning of the EU in cyberspace, which is considered to be „limitles"? And in general, can the digital sovereignty of the EU be considered as a simple digitalization of Westphalian sovereignty, and digital space – as a new dimension of territory (along with land, water and air spaces)? The practice of international law shows that with the development of international relations, it is not the category of territory that changes, but rather its substantive aspect. We believe that it is not necessary to deny the importance of the territory as the legal basis for the exercise of sovereignty in cyberspace, but rather to rethink the content of this category in the digital world. This is especially important in conditions when the EU puts the issue of digital sovereignty as the basis of its digital policy on its political agenda.

At the same time, just rethinking the category of territory is not enough to determine the boundaries of the EU's digital sovereignty: it is necessary to understand, on the basis of what principle should the borders of the EU territory be determined in cyberspace. We should not forget, that the development of the category of territory in international law has always been based on a certain principle. For example, when water and air spaces were included in the category of territory, the land space, on which the State is located, was considered as such a principle (for example, when determining the height or width of the extension of the sovereignty of the State), while in the case of diplomatic and consular missions, water and aircrafts, scientific stations in Antarctica and/or space objects, the principle of flag was considered as the basis. Moreover, in the conditions of scientific and technological development in the field of outer space research, when it became possible to fly into outer space, spaceships and other outer space objects also began to be considered as a territory, whose provisions

[36] *Barcelona Traction (Belgium v. Spain)*. Judgment. International Court of Justice. 5 February 1970. General List no. 50 [online]. Available at: https://www.icj-cij.org/public/files/case-related/50/050-19640724-JUD-01-00-EN.pdf

[37] BARTELSON J. *A Genealogy of Sovereignty*. Cambridge: Cambridge University Press, 1995, pp. 26.

on jurisdiction are specified in the Treaty on Outer Space (1967).[38] In this regard, the evolution of the content aspects of the territory at the expense of air, sea and outer space makes it possible to include new spaces in the category of territory, such as, for example, cyberspace.

However, unlike other categories of territory, cyberspace has a specific and multifaceted nature, which does not allow it to be viewed through the classical (Westphalian) understanding of the territory and the already existing principles for determining such a territory.[39] It is not difficult to notice that the classical territory, whether it is land, water or air, always has physically tangible and geographical boundaries, already given by nature, while in cyberspace, the subjects of the digital world themselves become the creator of such a territory and can create as many cyber territories as they please, for example, by developing new websites. In the conditions of its „limitless" nature, cyberspace becomes similar to outer space, only in contrast to the fact that at the current stage of the development of human civilization, the digital world is available to us, while the outer space is not yet. If we draw parallels, then the situation with the development of the digital world can be compared with the expansion of the territory of some European states (like Spain, Portugal and France) during the Age of Colonization at the expense of then unknown territories of America, Asia and Africa (i.e. *terra nullius* for Europeans). However, if in the offline world such a process of territorialization was easy, for example, through the principle of flag[40] ot through concluded international treaties between European Powers (such as Treaty of Tordesillas (1494)),[41] then in the online world, the situation is much more complicated not only geographically, but also subjectively.

In the above context, as M. Zook notes, the digital world („Internet") becomes an incentive for the development of „new geographies" of interaction between people and territories in technical, social, political, cultural, economic and other areas.[42] In such cases, the question naturally arises: how to determine the limits of EU jurisdiction in the „limitless" cyberspace, and what principle should underlie it? When trying to answer this question, a number of difficulties arise. For example, the problem is that cyberspace includes not only

[38] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967).

[39] GRAHAM, M. Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities? *The Geographical Journal.* 2013, vol. 179, no. 2, pp. 177–182.

[40] LUGARD, L. The Basis of the Claim for Colonies. *International Affairs*. 1936, vol. 15, no. 1, pp. 3–25.

[41] The Treaty of Tordesillas was signed in 1494 between Spain and Portugal on the division of spheres of influence in the colonial world.

[42] ZOOK, M. The Geographies of the Internet. *Annual Review of Information Science and Technology*. 2006, vol. 40, no. 1, pp. 52–64.

infrastructure, including servers, computers and/or communication cables, but also the „information field" that is created by such digital infrastructure. According to M. Finnemore and D.B. Hollis, one of the obvious starting points for states to extend control over relations in cyberspace is the material nature of a significant part of digital technologies, located in a certain territory, such as servers, submarine cables and so on.[431] That is, if we consider the cyberspace from this point of view (i.e. from the point of traditional (Westphalian) understanding of territory), the digital sovereignty will only cover material part of digital technologies, while the „information field" and data flow (i.e. digital world, created through such digital technologies) will remain outside regulation.[44] Besides, cyberspace, unlike other categories of territory, is no longer exclusive as in the case of Westphalian sovereignty, since not only states, but also BigTech companies (such as Google, Facebook, etc.) turn cyberspace into their „common" territory.[45] For example, such BigTech companies create business products, use cookies and softwares to collect data and conduct surveillance of data subjects, while states themselves delegate control of their laws to such companies, implementing their digital policies through such BigTech companies. All these are clear examples of drawing digital borders in cyberspace, which brings to the fore new risks and challenges, that are not known to the traditional (Westphalian) understanding of sovereignty.

We believe that in order to clearly understand the EU's digital sovereignty, it is necessary to determine, what quality the digital sovereignty gives to the EU, and which goal the EU is trying to achieve with this quality. However, the task is difficult here as well: the analysis of official EU documents shows that there is no unambiguous interpretation of the content of the term „digital sovereignty". For example, the European Parliament notes about *„establishing"*[46] of digital sovereignty, while the European Commission and the European Council emphasize *„defending"*[47] and

[43] FINNEMORE, M., HOLLIS, D. B. Constructing norms for global cybersecurity. *American Journal of International Law*. 2016, vol. 110, pp. 460.

[44] SCHMITT, M. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017, pp. 638 [online]. Available at: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9

[45] GÁBRIŠ, T., HAMUĽÁK, O. Pandemics in Cyberspace – Empire in Search of a Sovereign? *Baltic Journal of Law & Politics.* 2021, vol. 14, no. 1, pp.103–123.

[46] See: *EU institutions establish common priorities for 2021 and until next elections* [online]. Available at: https://www.europarl.europa.eu/news/en/press-room/20201217IPR94201/eu-institutions-establish-common-priorities-for-2021-and-until-next-elections)priorities-for-2021-and-until-next-elections

[47] See: *European Commission: Statement by the President at ‚Internet, a new human right.* [online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/statement_20_2001

„achieving"[48] of digital sovereignty, respectively. Based on the analysis of official documents of EU political institutions, it is very difficult to determine: does the EU already have digital sovereignty at the moment or is it still striving for it? Moreover, it is possible that the phenomenon of the EU's digital sovereignty, which is often mentioned by European politicians, is a „bluff" and currently has no practical legal basis, but only serves to „intimidate" other digital partners through data protection instruments (such as GDPR, DGA, etc.) in order to protect by the EU its „weak" position and interests in the digital world.

Nevertheless, we can state that the developement of the EU's digital sovereignty takes place in the context of a debatable, dynamic, constantly changing and uncertain paradigm of the international system. Most likely, it is precisely because of such uncertainty that the EU uses broad and fictitious links with the territory in its data protection instruments in order to have convenient levers of influence at hand in the digital world in the event of the development of various unpredicted scenarios in the future. In particular, this can be seen in the very designation of the scope of application of the GDPR: article 3(2) of the GDPR states that the Regulation applies to data controllers and processors that are not established in the EU, if they process data related to the offer of goods or services to data subjects in the EU or monitor their behavior in the EU. Thus, the EU finds a way to exercise its sovereign power that is not based on the concept of geographical territory. Moreover, both the GDPR, and the DSA[49] and the DMA,[50] the expression *„in the Union"* is often used, which may imply a territory, and not necessarily a physical one.[51] Thus, the EU so far relies on the flexibility of interpretation of its provisions in the event of various unforeseen situations in the digital world, but such uncertainty not only exacerbates the existing „digital chaos", but also does not provide any effective and practical solution for the EU in the long-term vision.

---

[48] See: *European Council: Remarks by President Charles Michel after the Special European Council meeting on*. [online]. Available at:-https://www.consilium.europa.eu/en/press/press-releases/2020/10/03/remarks-by-president-charles-michel-after-the-special-european-council-meeting-on-2-october-2020/

[49] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) (Hereinafter – DSA).

[50] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) (Hereinafter – „DMA").

[51] For example, the AG, in the opinion of the *Salemink* case, argued that: *„(…) for EU purposes, the ‚territory' of the Member States is the area (not necessarily territorial, in the spatial or geographical sense) of exercise of the competences of the Union"* // See: Opinion of Advocate General Cruz Villalón delivered on 8 September 2011 in the case of *A. Salemink v Raad Van Bestuur Van Het Uitvoeringsinstituut Werknemersverzekeringen*. (Case C-347/10) p. 54.

4. The EU's dependence on foreign technologies and the lack of investments as the main obstacles to the implementation of the EU's digital sovereignty in the field of data governance.

In addition to the above-mentioned issues of a unified and clear understanding of the concept of digital sovereignty of the EU, nowadays the successful implementation of the EU digital policy is hindered by the high degree of dependence of Europeans on foreign digital services and technologies, as well as the lack of investments in the digital sector (compared to other technologically advanced states).[52] As B. Thieulin notes: „In terms of investments, the GAFAM (…) hold significant weight with €46.6 billion invested by the top 20 digital companies in the world during the first quarter of 2018, including € 32.5 billion by the GAFAM alone, primarily in the field of cloud computing (data centres). Opposite this strike force, there are no European digital operators among the leading global companies in the sector, nor are there any occupying a privileged position in any of its segments (…)".[53]

Indeed, the digital market is increasingly dominated by foreign companies, mainly from the USA and China, which may control quite large segments of digital technologies. In this regard, the European Parliament sees concerns about the role of Chinese companies in the European 5G market and the aggravating dependence of the EU on equipment suppliers from USA, China and other countries. For example, as noted in one of the official documents of the European Parliament: „With a global market share of 29 %, in 2018 nominally private Huawei Technologies ranked first among the top seven global telecoms equipment vendors, ahead of American Cisco and Ciena, Swedish Ericsson, Finnish Nokia, South Korean Samsung and Chinese state-owned ZTE Corporation. Huawei and ZTE are national champions that have benefited both from being shielded from foreign competition by means of domestic market access barriers and from indigenous innovation policies rolled out since 2006."[54] Such concerns on the part of the European authorities are not unfounded: nowadays delays for the EU in

[52] AUTOLITANO, S., PAWLOWSKA, A. Europe's quest for digital sovereignty: GAIA-X as a case study. *IAI Papers*. 2021, vol. 21, no. 14, pp. 1–22.

[53] THIEULIN, B. *Towards a European digital sovereignty policy* [online]. Available at: https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf

[54] GRIEGER, G. *5G in the EU and Chinese telecoms suppliers* [online]. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf

the transition to 5G infrastructure significantly increases the technological gap of the EU from other digital leaders. This, in turn, naturally leaves its negative imprint on the profitability of private investors' investments in the EU's digital sector. At the same time, the concerns expressed are not limited to the 5G market only. Another example of the EU's digital dependence on foreign companies is the use of cloud technologies. In this area, EU Member States are deprived of the ability to control the data of their citizens transmitted through cloud services, since such data mainly falls, for example, under the jurisdiction of the USA. In this regard, B. Thieulin clearly emphasize that „(t)his sector's unbalanced situation, which is sometimes described as a „colonisation" of the European digital market by major American platforms, is a huge risk for the EU's economy, but also for its workers and citizens who only benefit from a limited offer. The first risk is that of witnessing obstacles to competition that are likely to arise from an oligopolistic situation.[55] This, in turn, creates the risk of a conflict of jurisdictions in the digital world between different subjects of the digital market.

As one can see, the above problems are directly related to the weak role of European companies (compared to companies in China and the USA) in the global digital market. In particular, according to the research of A. Aktoudianakis: „There is currently insufficient European competition in the cloud sector. The global cloud storage services market is largely dominated by US and Asian companies. The leaders in this market are Amazon (45%), Microsoft (17.9%), Alibaba (9.1%), Google (5.3%), and Tencent (2.8%). While an estimated 92 % of data produced in the West is currently located in the US, only 4% is stored in Europe."[56]

Understanding the seriousness of existing risks, the European Commission is developing a strategy to address the above problems by implementing a number of initiatives within the framework of the European Data Strategy. It should be noted that the main goal of the European Commission in this area is to ensure the free transfer of data through the EU Member States in accordance with European rules and standards, concerning, in particular, privacy and data protection.[57] In addition, in the context of strengthening the EU's potential in the field of cloud technologies, it is impossible not to mention the European initiative of

[55] =THIEULIN, B. *Towards a European digital sovereignty policy* [online]. Available at: https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf

[56] AKTOUDIANAKIS, A. *Fostering Europe's Strategic Autonomy: Digital sovereignty for growth, rules and cooperation* [online]. Available at: https://www.epc.eu/content/PDF/2020/Digital_SA_paper_EPC_and_KAS.pdf

[57] See: *European Commission: A European Data Strategy (COM/2020/66)* [online]. Available at: lex.europa.eu/legal- content/IT/TXT/?uri=CELEX:52020DC0102

GAIA-X – a non-profit organization, the members of which are not only cloud service providers, but also ordinary users. The goal of this project is to create universal information spaces designed for users who want to share their business data. In order to achieve this goal, a number of partners (including American and Chinese companies) contribute to the GAIA-X project, although it is assumed that each participating company should be based in the EU. With the successful implementation of the GAIA-X project, any user will have the opportunity to access to their data without switching between different cloud service providers. This is the main goal of the GAIA-X project – to ensure the maximum possible compatibility and expand the existing data transfer capabilities between various cloud services.[58] Although the project itself is still in the process of development, which according to some experts „is stuck in the concept stage".[59] However, it will be possible to assess how successful such initiatives will be only after a certain period of time and accumulation of new cases in the future.

At the same time, the above-mentioned initiatives cannot be analysed and implemented outside the international aspect. In order to be effective in the field of global data governance, the global data economy requires mutual trust between its parties, and in the existing conditions it is clearly not enough. The practice shows that conceptual differences often lead to serious conflicts between data governance and protection regimes, such as between the EU and the US in the context of the transatlantic *Privacy Shield* agreement. In particular, in the case of *Schrems II* the Court held that *Privacy Shield* is not effective and sufficient mechanism to guarantee the rights of EU citizens to protect their personal data.[60] Undoubtedly, this judgment will negatively affect not only EU citizens, but also most European companies that have used *Privacy Shield* in recent years in order to exchange data with their partners from the USA. As one can see, this judgment has made the „dialogue" between the USA and the EU in the field of data protection even more difficult. Moreover, the Court did not just invalidate the *Privacy Shield* agreement: it also formulated so-called „standard contractual clauses",[61] establishing contractual obligations for both parties to facilitate the transfer of necessary data to their foreign partners. It means that the parties will be obliged to monitor the compliance of the data transmission

[58] See: *What is Gaia-X* [online]. Available at: <https://gaia-x.eu/what-is-gaia-x

[59] VASKE, H. *European cloud project Gaia-X is stuck in the concept stage* [online]. Available at: https://www.cio.com/article/308818/european-cloud-project-gaia-x-is-stuck-in-the-concept-stage.html

[60] See: Case C-311/18. *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*. Judgment of the Court (Grand Chamber) of 16 July 2020 [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311

[61] Ibid.

systems and tools they use with the new European standards, specified in the judgment of the Court.[62]

The Court's jugdment in the *Schrems II* case created new aggravating conditions for the transatlantic partners. The point is that before transferring data, such partners must ensure by themselves that the data exchange complies with the requirements of the EU „standard contractual clauses", which requires partners to analyse both the US and EU data protection laws. We believe that the Court's judgment in the *Schrems II* case will definitely have a serious impact on transatlantic private-legal relations: they will not only force partners to introduce huge resources into the analysis of the EU and US data protection laws, but also reduce the competitiveness of European companies, operating in both the EU and US digital markets. In addition, another aspect that significantly restricts international data exchange both on a global and regional level is the trend towards data localization. Nowadays in a number of countries data localization laws are already in effect.[63] Such localization may be a consequence of the policy measures taken, which either significantly burden the data transfer process or make it impossible.

All the above aspects make us skeptical about the possibility of practical implementation of the concept of global data governance, which, in turn, shows „immaturity" in conditions of mutual distrust of subjects among themselves, for whom their own political and economic interests take precedence over the possibilities of mutually beneficial international cooperation. In such a situation, there can be no winners, and states, including the EU, should understand that only through international consensus will be possible to clearly draw the capabilities and borders of states among themselves in the digital world and achieve a universal practical result (as, for example, it became possible through the Treaty of Westphalia), otherwise the development of different adverse scenarios, even up to information wars between states, on the one hand, and BigTech companies, on the other, while human rights, including personal data, will turn out to be a „weapon" in the hands of the parties and will be deprived of protection.

[62] POLITO, C. La governance globale dei dati e la sovranità digitale europea. *IAI Papers.* 2021, vol. 21, no. 11, pp. 1–12.

[63] GUSEYVA, V. *Data Residency Laws by Country: An Overview* [online]. Available at: https://incountry.com/blog/data-residency-laws-by-country-overview

5. The model of multilateral participation as the only optimal solution?

As noted above, there is no single global system for data governance and protection as such, and nowadays the digital world is characterized by political fragmentation and the desire to influence the digital economy as much as possible by strengthening their own positions. It is easy to see how one digital leader is trying to restrain the growth and influence of another digital leader in the modern digital world by all possible means (including economic sanctions, countermeasures and/or trade wars). The tense economic relations between the USA and China is a good example. In particular, the recent political tension between the two economic (digital) giants occurred due to heavy taxes, imposed by the US government the on imports of goods from China. To this, the Chinese government responded with the same counter-measure, also imposing the same import taxes on goods against the USA.[64]

The above-mentioned example of the tense trade relations between the USA and China clearly shows the current political and economic situation in the international arena. At the same time, American and Chinese BigTech companies that are leaders in both information technology and data control, are increasingly using their economic and technological advantages to strengthen their positions in the field of political relations. In such conditions, a new model of multilateral and consensual participation is considered as an optimal solution for the digital sector.[65] Within the framework of this model, states (including the EU) should pay attention not only to the needs and interests of other states, but also private sector companies in order to achieve mutually beneficial and effective cooperation.[66] We should not forget, that nowadays BigTech companies have a significant influence on global digital economy, so it is impossible not to take into account their interests when searching for solutions. At the same time, we also consider it important that such a model should not neutralize the role of states (including the EU) in the digital world: it is highly undesirable that the interests of the private sector take precedence over the interests of sovereign States, since it is the main task of states is to ensure human rights in the digital sector. We believe that such a model can help to avoid the Hobbesian scenario on *bellum omnia contra omnes*,[67] focused on digital realities. One should not forget, that

[64] FAJGELBAUM, P. D., KHANDELWAL, A. K. The Economic Impacts of the US–China Trade War. *Annual Review of Economics*. 2022, vol. 14, no. 1, pp. 1–28.

[65] POLITO, C. La governance globale dei dati e la sovranità digitale europea. *IAI Papers*. 2021, Vol. 21, No. 11, pp. 1–12.

[66] Ibid.

[67] HOBBES, T. *Leviathan*. Hamburg: Meiner Verlag. Philosophische Bibliothek. 2005, pp. 610.

there cannot be a single winner in the world of digital economy, because all its parties are interconnected.

6. Conclusion

The EU's attempts to assert its digital sovereignty in the digital sphere face the following obvious challenges: *1) the ambiguity of understanding the EU's digital sovereignty*, *2) the EU's increasing dependence on foreign digital services and technologies* and *3) the lack of investments in the EU's digital sector*. Taking into account these obstacles, the EU is trying to overcome them by developing its digital strategies, as well as by flexibility in the interpretation of its data protection laws, where the case-law of the CJEU plays a significant role. However, the effectiveness of the EU strategies can only be assessed in the future perspectives, since it is not „mature" enough yet.

The study shows that in the existing situation all the parties of the digital world (including the EU) are in a „no-win" situation, and over time this situation is only getting worse as each of them tries to establish their hegemony in the digital economy (for example, as in the case of trading wars between the USA and China). We believe it is high time to seriously think about a new „digital Westphal" system, only in the conditions of which it will be possible to avoid future digital cataclysms and informational wars between the leading subjects. It seems that for effective governance of the digital sector, it is necessary to use an approach involving the widest possible range of subjects interested in defining common rules for ensuring free data flow based on mutual trust at the global level.

However, the new system should not reduce the role of the state (including the EU) in regulating digital market. In the conditions of „digital chaos", the state should play the fundamental role in the digital sector. We should not forget, that only the states (including the EU) can ultimately protect the rights and legitimate interests of their citizens as the real guarantors of the protection of human rights in the digital world.

List of references

AUTOLITANO, S., PAWLOWSKA, A. Europe's quest for digital sovereignty: GAIA-X as a case study. *IAI Papers*. 2021, vol. 21, no. 14, pp. 1–22 [online]. Available at: https://www.iai.it/en/pubblicazioni/europes-quest-digital-sovereignty-gaia-x-case-study

BARTELSON J. *A Genealogy of Sovereignty*. Cambridge: Cambridge University Press, 1995 [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843913

BELLANOVA, R., CARRAPICO, H., DUEZ, D. Digital/sovereignty and European security integration: an introduction. *European Security*. 2022, vol. 31, no. 3, pp. 337–355 [online]. Available at: https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2101887

COUTURE, S., TOUPIN, S. What does the notion of „sovereignty" mean when referring to the digital? *New Media & Society*. 2019, vol. 21, no. 10, pp. 2305–2322 [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107272

DI STASI. A. The Enlargement of Competences of the European Union between State Sovereignty and the so-called European Sovereignty: Focus on the Limits of Applicability of the Charter of Fundamental Rights of the European Union. *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*. 2020, vol. 22, no. 45, pp. 131–154 [online]. Available at: https://www.redalyc.org/journal/282/28268121007/html/

FAJGELBAUM, P. D., KHANDELWAL, A. K. The Economic Impacts of the US–China Trade War. *Annual Review of Economics*. 2022, vol. 14, no. 1, pp. 1–28 [online]. Available at: http://www.econ.ucla.edu/pfajgelbaum/tradewar_1203.pdf

FISCHER, D. The digital sovereignty trick: why the sovereignty discourse fails to address the structural dependencies of digital capitalism in the global south. *Z Politikwiss.* 2022, vol. 32, pp. 383–402 [online]. Available at: https://link.springer.com/article/10.1007/s41358-022-00316-4#citeas

GÁBRIŠ, T., HAMUĽÁK, O. 5G and Digital Sovereignty of the EU: The Slovak Way. *TalTech Journal of European Studies*. 2021, vol. 11, no. 2, pp. 25–47 [online]. Available at: https://sciendo.com/article/10.2478/bjes-2021-0013

GÁBRIŠ, T., HAMUĽÁK, O. Pandemics in Cyberspace – Empire in Search of a Sovereign? *Baltic Journal of Law & Politics.* 2021, vol. 14, no. 1, pp. 103–123 [online]. Available at: https://sciendo.com/article/10.2478/bjes-2021-0013

GOLDSMITH, J., WU, T. (ed.). *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press. 2006, pp. 238.

GRAHAM, M. Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities? *The Geographical Journal.* 2013, vol. 179, no. 2, pp. 177–182.

HAMUĽÁK, O. „Lessons from the Constitutional Mythology" or How to Reconcile the Concept of State Sovereignty with European Integration. *DANUBE: Law and Economics Review.* 2015, vol. 6, no. 2, pp. 75–90.

HOBBES, T. *Leviathan*. Hamburg: Meiner Verlag. *Philosophische Bibliothek*. 2005, pp. 610.

KOCHARYAN, H., VARDANYAN, L., HAMUĽÁK, O., KERIKMÄE, T. Critical Views on the Right to Be Forgotten After the Entry Into Force of the GDPR: Is it Able to Effectively Ensure Our Privacy? *International and Comparative Law Review*. 2021, vol. 21, no. 2, pp. 96–115.

LAUTERPACHT, H. *Recognition in International Law*. Cambridge: Cambridge University Press. 2012, pp. 419.

LUGARD, L. The Basis of the Claim for Colonies. *International Affairs (Royal Institute of International Affairs 1931–1939)*, vol. 15, no. 1, 1936, pp. 3–25.

PEROČEVIĆ, K. European Union Legal Nature: EU As Sui Generis – A Platypus-Like Society. *Inter EU Law East*. 2017, vol. 4, no. 2, pp. 101–116.
POHLE, J., THIEL, T. Digital sovereignty. *Internet Policy Review*. 2020, vol. 9, no. 4, pp. 1–19.
POLITO, C. La governance globale dei dati e la sovranità digitale europea. *IAI Papers.* 2021, vol. 21, no. 11, pp. 1–12.
ROBERTS, H., COWL, J., CASONARI, F, MORLEY, J., TADDEO, M., FLORIDI, M. Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies. *Internet Policy Review*, Forthcoming, 2021, pp. 1–26.
RUOHONEN, J. The Treachery of Images in the Digital Sovereignty Debate. *Minds & Machines*. 2021, vol. 31, pp.439–456.
SCHIA,-N.,-GJESVIK,-L. China's-cyber-sovereignty. *NUPI. Policy Brief.* 2017, vol. 2, pp. 1–4.
SCHMITT, M. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. 2017, pp. 638.
THIEL, T. Unendliche Weiten? Umkämpfte Grenzen Im Internet. *INDES – Zeitschrift für Politik und Gesellschaft*. 2012, vol. 1, no. 4, pp. 61–67.
ZOOK, M. The Geographies of the Internet. *Annual Review of Information Science and Technology*. 2006, vol. 40. no. 1, pp. 52–64.

Court decisions

Barcelona Traction (*Belgium v. Spain*) Judgment. International Court Of Justice. 5 February 1970. General List No. 50.
Case C-18/18 – *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, Judgment of the Court (Third Chamber) of 3 October 2019.
Case C-311/18 – *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*. Judgment of the Court (Grand Chamber) of 16 July 2020
Island of Palmas (*Netherlands v. USA*). 4 April 1928. Volume II pp. 829–871 [online]. Available at: https://legal.un.org/riaa/cases/vol_II/829-871.pdf

Other sources

Convention on Rights and Duties of States Signed at Montevideo on December 26, 1933 (Montevideo Convention)
Convention on International Civil Aviation, signed at Chicago, on 7 December 1944 (Chicago Convention)
Draft declaration on rights and duties of states. General Assembly resolution 375 (IV) of 6 December 1949
*European Commission: A European Data Strategy (COM/*2020*/66), 19 February 2020* [online]. Available at: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020DC0102
European Commission: Statement by the President at ‚Internet, a new human right' [online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/statement_20_2001

European Council: Remarks by President Charles Michel after the Special European Council meeting on [online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2020/10/03/remarks-by-president-charles-michel-after-the-special-european-council-meeting-on-2-october-2020/

European Parliament: EU institutions establish common priorities for 2021 and until next elections [online]. Available at: https://www.europarl.europa.eu/news/en/press-room/20201217IPR94201/eu-institutions-establish-common-priorities-for-2021-and-until-next-elections)priorities-for-2021-and-until-next-elections

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (hereinafter – AIA)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (hereinafter – GDPR)

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) (Hereinafter – „DMA")

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) (Hereinafter – „DSA")

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) (hereinafter – DGA)

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967)

United Nations Convention on the Law of the Sea of 10 December 1982