CICERO FOUNDATION GREAT DEBATE PAPER

No. 25/01

January 2025

THE EU AND AI

THE NEED FOR THE EU'S POLITICAL TRANSFORMATION IN ORDER TO OBTAIN AI SOVEREIGNTY

GEORGIOS I. ZEKOS

International Hellenic University
Serres, Macedonia
Greece

Cicero Foundation Great Debate Paper No. 25/01

The Cicero Foundation is an independent pro-Atlantic and pro-EU think tank, founded in 1992 in Maastricht at the signing of the Maastricht Treaty.

www.cicerofoundation.org

The EU and AI

The need for the EU's political transformation in order to obtain AI sovereignty

Georgios I. Zekos *

zekosg@ihu.gr

1. Introduction

Globalization is lifting relationships out of the firmly territorial into the "global" or meta-territorial which means that the space in which social relations are conducted changes and so the manner of regulating those relations changes as well. In addition, globalization has both direct and indirect impact on states affecting the laws of international business transactions either negatively or positively. Moreover, globalization elevate the required government regulation of market affairs and so the liberalization and global integration of markets sets a reliant political initiative. Apparently, the power of sovereignty from the state is step by step shifting to market forces in a globalized world giving rise to different norms, standards and rules to cope with globalization.

The centrality of corporations' internationalization strategies to the evolving pattern of the industrial and investment processes of globalization became more and more noticeable. Legal systems become more and more permeable to external influences. Globalization not only increases the demands for organizational change but also the ethical challenges leaders face[1] or challenges to the established ethical principles/doctrines/rationale. In many countries, governments and people have

utilized globalization in a good way of improving all infrastructures etc. On the other hand, many states due to ideological attitudes have missed the chance to improve their economies and so their political status on the globe. Besides, the general destruction of climate via reckless utilization of resources due to globalization is one of the cons of globalization. It has to be taken into account that sustainable development is the opportunity for a globalizing society via justice which could be achieved by the development of an AAI digital economy run in an objective way rather than AI technology utilized by the current forces to keep their own status unchanged in the new AAI world.

Cyberspace is growing at a tempo that outpaces any modern medium of communication. As presently organized, cyberspace depends on a fixed technical infrastructure. It is characteristic that Cyberspace is profoundly and fundamentally different from "real space[2]". It could be said that the notion of cyberspace as "lawless" implies that there are legal gaps, but law deals with matters of cyberspace activity and it has expediated the expansion of private power[3]. Moreover, Cyberspace brings forward the electronic state sovereign based on state cyberspace territory denoting a new dimension into the utility of territory and state sovereignty[4]. In general, advanced electronic technology can be used in order to paralyze an inferior technology of a state and therefore threatening practically its sovereignty[5]. Networks are replacing hierarchies and markets as a basic form of economic organization.

Cyberspace is characterized as "a-territorial" with the conventional understanding of territory but cyberspace creates the notion of cyber-territory. To that extent, the emergence of AI technology has generated the AI cyber-territory. Moreover, AI embraces the capacity of a technology to perform intelligence functions such as perceiving, reasoning, learning, interacting with the environment, problem-solving, and exercising creativity.

Digitalization plays a key role in dropping the costs of engaging in international trade. Hence, digital connectivity and digital trade policies have a direct influence on the capacity to order and to deliver trade digitally. Undeniably, digitalization and digital

trade policies diminish overall trade costs at the border facilitating new trading opportunities[6]. Furthermore, Cyberspace and AI has empowered the emergence of digital globalization embraced by the endless cyber territory and, consequently, digital sovereignty of states. The new digital globalization brought a new intersection between international political economy, socioeconomic development, and innovation. It seems that the new digital globalization brings forwards new economic superpowers seizing an ever more momentous role in the global AI economy. New corporations or the old ones found themselves at center of new production processes by utilizing AI systems and capitalizing on ever more adaptable strategies to overcome their competitors. Of course, digital-globalization is still shaping via the utilization of AI technologies and so its final shape will emerge by the implementation of the forthcoming AAI technology run by AAI humanoids.

International and global governance rations are boosting the safe, trustworthy, and interoperable use of AI technologies and so industry players have been promoting greater consistency and interoperability via the advance of technical standards in bodies such as ISO[7]. It is worth noting here that globalization has caused a shift in law-making institutions and processes not mentioning the impact of AI technology on dealing with security problems in a digitalized globe penetrating any essence of conventional territory and security via technology given that most of the current transactions and activities take place via new technologies and so AAI systems will contribute in safeguarding the digital economy and its security.

Aim of this work is to present the necessity for the transformation of the EU into USE in order to survive in the AI globalized world. Has the decision of enlarging the EU achieved any political value in generating a strong political entity as a global player in the AI era or merely postponed the need of EU becoming a single political entity in order not only to avert major economic problems but also to end the forthcoming demolition?

2. State's Control over Cyberspace

Cyberspace was initiated by the State, and soon after was privatized and so the State minimized its straight connection in the information environment and more and more abandoned its role in running the Internet but not cyberspace and electronic networking in a broad sense. At the beginning the Internet was considered to be an international innovation lying beyond the reach of laws of any specific government[8]. On the other hand, the advance of cyberspace has challenged the law as new technologies characteristically do and the dilemma is whether to modify old legal doctrines in order to deal more effectively with the new reality or to acquire expressly tailored new doctrines.[9] It has to be taken into account that inventiveness does not forgive cyberspace technologies from conformity with the law[10]. Thus, cyberspace is still not above the law, whether on an International or national level[11].

Cyberspace is a network, which grew, suddenly, into a global network of networks, challenging the State's capacity to govern. It is vital for states to control the distribution of information. Governments maintain ownership over information exchange systems so as to preserve their control over ways of exchanging and disseminating information. To that extent, the digital/electronic environment makes possible the establishment of monopolies that gain their monopoly status by controlling technological standards[12].

It is worth noting that technological change has weakened the efficacy of State regulation, making it almost unfeasible for regulators to keep up with a technology that reinvents itself constantly. The majority of states use output access providers for filtering or blocking cyberspace content on its way to the end user. Hence, the State as a regulator constitutes a system of rules and so delivering rules for resolving conflicts and protecting rights or advancing policy objects through the legal system[13].

The erosion of state sovereignty is affected by globalization taking power from the state and giving it into the hands of other international players such as MNEs, NGOs or international organizations. The development of the electronic networking is destroying the connection between real world location and the authority of a local sovereign's efforts to regulate electronic global phenomena. Electronic/digital activities

that even modestly affect the critical interests of sovereigns are becoming subject of regulation by sovereigns[14].

On the one hand, cyberspace cut across territorial borders, creating a new land of human activity and undermining the practicability and legitimacy of applying laws based on geographic borders. On the other hand, all law is prima facie territorial[15] enclosing cyber-territory for purely electronic transactions. If sovereignty defined as the "final authority within a given territory", then the escalation of internalization via cyberspace transactions will have supplementary important implications for State sovereignty.

3. Law & Cyberspace

In fact, cyberspace disrupts existing power relationships and enables new ones. On the other hand, the market, norms, law, architecture[16] and their interactions regulate cyberspace. Global space is produced by the interconnectivity of cyberspace over "real" space, and by the interpenetration of the two which means that cyberspace extends further than the boundaries of any of the states, and the effects of any individual state regulation similarly spills over that state's borders[17]. As a result, the extensive availability of cyberspace has changed the character of commerce and communication.

Jurisdiction is related to the assumption that nation-states defined by fixed territorial borders remain the relevant jurisdictional entities, without any discussion of how people really experience allegiance to community or understand their relationship to geographical distance and territorial borders.[18] Current rules for jurisdiction and conflict of laws are territorially-based and were developed in an era when physical geography was more consequential than it is today. The idea of territoriality itself can be seen as a geographic strategy to control people and things by controlling area. The territorial principle is believed to be the foundation of global jurisdictional order, with other principles—extraterritorial jurisdiction—needing explicit justification to subordinate the territorial principle.[19] Simultaneously, the subsistence of a range of principles of jurisdiction makes certain that at least *one* State's regulation will apply.[20]

Personal jurisdiction doctrine offers instantiations of due process in any legal system[21]. Moreover, personal jurisdiction doctrine is not just as about the power of a court over a defendant but also as a final decision regarding choice of forum[22]. Additionally, the Court found that the basis of jurisdiction grounded on physical presence was enough to maintain personal jurisdiction, regardless of a Shoe minimum contacts analysis[23]. It is characteristic that the Supreme Court mentioned that defendant Goodyear did not object to the affirmation of personal jurisdiction in North Carolina regardless of the fact that it was not incorporated or headquartered there, and the litigation had no connection with the state of North Carolina, as the underlying incident had occurred in France[24]. Also, the Court upheld personal jurisdiction over railroad company Norfolk Southern in Pennsylvania, where plaintiff Robert Mallory had chosen to sue[25].

Can the principle of territoriality be applied to cyberspace if it is considered as state's cyber territory? The territoriality principle lies at the very centre of any legislative endeavor of the state within its territory. As a result, the implementation of jurisdictional competences is above all a territorial happening (*ratione loci*). State competences come to life in a specific space and continue bound exclusively thereto. Taking into consideration that the issue of jurisdiction is entangled with precisely the fixed conception of territorial boundaries, territorially-based sovereigns are facing challenges regulating in an electronic/cyber/virtual environment. The EU recognized that cyberspace performance can and even has to be regulated in order to find an equilibrium between freedom and control[26].

Cyberspace does not challenge the territorial notion of the state as a collective organization that resides within specific geographical borders but merely the electronic state sovereign based on state cyberspace territory brings a new dimension into the utility of territory and state sovereignty. The exclusivity of sovereign authority, to the exclusion of external forces, is rooted in the relationship between physical proximity and the effects of any particular behavior which with the emergence of the electronic state sovereign expands its applicability into electronic transactions that finally get again a physical proximity with territorial effects. A nation's prerogative to control

events within its territory entails the authority to regulate the national effects of extraterritorial acts including the harmful local effects of electronic activity. Thus, cyberspace activities originating outside the territory but having an effect upon people within the territory of a state are potentially subject to the claims of the sovereign. It should be taken into consideration that the territorial jurisdiction of states and the jurisdictional limits of the municipal courts are still based on the territorial theory.

It has to be taken into account that cyberspace, altogether, is an international cyber-"territory." Moreover, The International Law Commission of the United Nations refers to the concept of 'extraterritorial jurisdiction', defining it as 'an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the State in the absence of such regulation under international law[27]'. As mentioned earlier, the application of law is territorial[28].

4. Defining State Sovereignty

The territoriality doctrine under international law assigns to states plenary jurisdiction over all matters that fall within their territorial sovereignty. Sovereignty denotes the "totality of international rights and duties recognized by international law"[29] as residing in an autonomous territorial unit—the State. Moreover, sovereignty is related only to the basis of legitimate authority within a state. To that extent, Krasner[30] views sovereignty as a supposed limitation on states' power to interfere in each other's affairs. Sovereign nation state is an entity whose sovereignty jointly derives from the sole jurisdiction to make laws for its people and its freedom from the coercive authority of any other state[31]. Moreover, the state lies upon the foundation of sovereignty, which expresses internally in the supremacy of the governmental institutions and externally as the supremacy of the state as a legal person[32]. The courts derive its power to adjudicate a matter from the state. Therefore, the concept of jurisdiction is based on the concept of state.

Sovereignty resides in that political body known as the state and so Sovereignty is a quality of statehood. Internal political ordering is an underlying feature of state sovereignty[33] and the legitimacy of a specific exercise of political power is a question of legality. Moreover, a state has authority to regulate the transmittal of information across its borders and the use of that information by individuals within its territory[34]. States rely on the territoriality principle to regulate in-state hardware and software used in cyberspace communications. Moreover, state control is fundamental of state sovereignty[35]. As mentioned earlier, the state has taken control of cyberspace transactions having effects upon its people and so it considers cyber- territory as part of its own territory. On the one hand, cyberspace and electronic networking can be seen as a post-national situation[36].

The concepts, doctrines, and laws related to national sovereignty should be directly applicable to electronic national sovereignty as well. Zekos considers that the intention to produce an outcome via the utilization of cyberspace and the location of servers that conduct electronic transactions could be the factors determining jurisdiction for cyberspace transactions. In this way, not only will servers be careful to follow the law for electronic transactions and therefore take all necessary precautions to protect the electronic system from illegal intrusions and illegal uses, but also, people utilizing specific servers will have certainty about the jurisdiction in case of problems or any illegal electronic transactions taking place. Universal cyber-jurisdiction will mean that any nation whose people are affected in any way by an electronic action will have jurisdiction to decide, and the decision will be enforced by an international convention of enforcement of foreign courts decisions. The universal cyber-jurisdiction will be especially useful for criminal and intellectual property cases[37]. The establishment of national cyber-courts having universal cyber-jurisdiction dealing with acts that take place within nations' cyber-territories will bring efficiency to the globalized economy and to the world.

Electronic state sovereignty and territory can be infinite in an electronic dimension covering any possible electronic space anywhere the electronic signals transferring information travel before received by electronic means located within the territory of

a state on earth. A state that possesses the most advanced and original technology can intervene and control the cyber-territory of any state as long as there is no possibility to block electronically the intervention in the cyberspace of any state. Therefore, the problem according to Zekos lies in the fact that the state with supreme electronic technology will establish a more advanced electronic/cyber/virtual state sovereignty rather other less advanced state and so overtaking/ engulfing electronic transactions and capabilities. In fact, electronically independent states will impose the new decision-making order to other states less electronically independent. The nature and depth of the electronic state sovereignty of being an endless electronic space depending on the electronic capacity and capabilities of a state accessible from the state sovereignty by the use of electronic technology and not only cyberspace under its current conception might cause frequent conflicts among states because of the overlapping and the fact that electronic actions concurrently affect a number of jurisdictions and so there is a need for an international clarification of some international law principles of non-intervention in order to be applicable in a state's cyber-territory and so state's electronic/cyber/virtual sovereignty. Thus, cyber state sovereignty should be the term for the entirety of international rights and duties that should be recognized by international law regarding this new dimension of the state's sovereignty. Taking into consideration the depth of the use of electronic technology in the states' affairs and their citizens' lives, electronic intrusion of the cyber state sovereignty by the use of electronic technology will make the state sovereignty an empty letter because everything will be controlled and influenced by the used technology from a distance. This means that in the future the conquest of a state from a distance via electronic technology cannot be excluded, which makes the defense of state sovereignty an empty letter and emphasizes the need ofl the defense of the electronic state sovereignty.

Nonetheless, human relationships and interactions are taking place on cyberspace and so stretching the traditional notions into their cyber activities[38].Yassin Abdalla Abdelkarim[39] mentions that "Zekos noted that… cyber globalization created the concept of cyber sovereignty; it is an adaptation of the traditional legal notion of sovereignty in cyber-space… Consequently, states can impose their sovereignty over

electronic transactions and interactions that affect their interests. This elaboration proves the existence of cyber sovereignty as a legal notion." [40] How the demarcation of cyber borders is achieved? Can we have demarcation of cyber borders as long as cyber-states do not exist? At least under the human capabilities, cyber states cannot be understood and seen but the development of AAI humanoids having the ability to be transformed from material entities to cyber ones and vice versa the demarcation with an electronic way can be seen. Currently, the impact of electronic transaction is felt by people on earth mainly within the borders of a state which means that the state's jurisdiction on sovereignty will be applied. Thus, states' understanding and connection with cyber territory is materialized in order to be processed and understood via software and hardware located within the conventional territory.

5. AI & State Sovereignty

Will AAI generate AAI states? Is AI space part of state sovereignty? Does state sovereignty coincide with AI sovereignty ? Do AAI humanoids move in AAI sovereignty? Due to technology, States experience a sovereign identity calamity when their capacity to further collective effort, protect national cultural values, or govern spatially is critically disputed. Moreover, the state's identity is entrenched in a specific territorial location and included functional, ideational, and spatial components[41]. Also, states occupy physical territory on earth where their jurisdictional authority is broadly recognized. Political entities define and defend territorial borders keeping out unwelcome people, products, and various threats[42]. Moreover, states utilize territorial bordering technologies in exercising state authority and as a reply to challenges to state sovereignty. Also, nowadays states filter cyberspace traffic according to territory in order to preserve their sovereign identity[43].

Countries establish cyber-borders with laws, practices, and so cyberspace building planned to filter digital information within the territorial jurisdiction of the country. To that extent, new digital bordering methods imitate and reproduce the territorial identity of the country and so borders and territoriality, are prevalent in countries' official cyberspace language.

The use of territorial bordering technologies is deemed as a legitimate exercise of state authority and many states have the technological capability to filter cyberspace traffic according to territory. Functionally, countries[44] organize human efforts to accomplish collective goods, such as defense, education, public order, or economic development occupying physical territory on earth where their jurisdictional authority is largely accepted. Hence, no other authority in the modern world has territoriality as its defining feature[45]. Thus, countries have constantly found it difficult to govern effectively within their territorial borders. In line, Beth A. Simmons & Rachel A. Hulvey[46] argue that "that states can and do border the internet in ways that are mirrored at their geographic borders in the physical world… the sovereign identity crisis can be understood through the familiar concept and practice of bordering." It is characteristic that States segregate their territory from global information by blocking foreign websites rather than demanding the removal of specific content and so the blocking of foreign websites denotes wish of states to supervise how and where citizens are subjected to foreign ideas, products, and transactions[47].

6. AI & EU Politics

Has EU achieved the projection of collective power, wealth, and influence by becoming a global power? It seems that in its current form and due to the political approach of EU members, the European Union has managed partly the projection of collective power, wealth, and influence but not becoming a global power[48]. The political approach of EU in the Ukrainian crisis has shown the weakness of the current EU to act as a global player.

Will AI promote European integration? The development of AI and moreover the advanced AI will allow the automated decision making based on objectivity rather than subjectivity of the current human society. The utilization of AI technology on the level of decision making of EU commission will allow automated decision objectively on EU matters producing the best result rather than a subjective and calculated decision based more on national interests rather than maximizing the outcome for EU.

Will AI allow better decisions for EU policy? Have the European leaders all the data for a rightful decision for EU People without AI technology? EU leaders could have taken better decisions by using AI technology on matters of engagement of EU on various conflicts rather than nowadays not only by using incomplete data but also by subjectively promoting national interests rather than purely EU Interests. AI technology could have calculated all the elements concerning the engagement of EU on a conflict and have advised not taking part in a conflict which might be proven damaging for the EU economy.

Does the implementation of AI technology necessitate the transformation of EU into the United State of Europe? The expansion and advancement of AI technology and its utilization on all fields of human life will generate the need for a central government system in order to achieve the best outcome forcing a political integration and transformation of EU into the United State of Europe[49] acting as a global player antagonizing other super powers. Also, due to the European civilization, the United States of Europe will become the balancing global player bringing stability and growth on the global economy and so avoiding any global instability causing economic problems not only upon EU economy but also on global one as it seems to take place currently[50].

Has the EU involvement in Ukraine crisis caused any economic damages to all EU member States? The reality has revealed that energy has become more expensive for EU economy and so generating an increase on cost of production leading to big economic problems for all the economies of the EU Member States. Moreover, EU has not taken decisive political actions in order to safeguard its own interests objectively pinpointed. Has EU emerged as a global power due to its involvement in Ukraine? Has EU involvement in Ukraine crisis opened the door for another war on EU soil? In fact, it seems that EU has shown its political weaknesses which means that there is imminent obligation of EU Member states to reverse/ repeal the demolishing process in order to avoid many forthcoming disasters taking place in EU soil.

7. Autonomous AI Sovereignty: The Device of EU In Achieving Political Unity

Digital sovereignty is extended further than conventional sovereignty depended on the capacities of the technology utilized in accessing it but its access takes place via a server with a sovereignty and according to the technological capabilities[51]. Besides, N. Tsagourias and R. Buchan[52] refer to the lack of an inseparable bond between territory, sovereignty and jurisdiction by coupling the nature of sovereignty with the authorities of the state, but not with the territory.

Can a state survive without dealing with digital sovereignty? States occupy physical territory on earth where their jurisdictional authority is recognized and only states have territoriality as their defining feature[53]. It has to be taken into consideration that nowadays international order is still grounded on the territorial principle, but cross-border data flows question the traditional territorial grasp of sovereignty.

It is characteristic that boundaries and sovereignty are inseparably connected perceptions and so boundaries are not just physical but also take the form of conceptual and legal boundaries due to the domain of digital sovereignty. Due to the fact that states' authority alone is insufficient for successfully tackling many of the global challenges raised by AI, there is a need of establishing global governance mechanisms and so boosting state control over digital technologies unilaterally by declaring their sovereignty[54]. It has to be taken into account that the territorial bordering technologies are regarded as a legitimate exercise of state authority and so territorial bordering is a reaction to challenges to state sovereignty[55]. Digital infrastructures are different from traditional infrastructures owing to their capacity to collect, store, and make digital data available instantaneously across many systems[56]. To that extent, states border cyberspace in ways that their geographic borders in the physical world are reaffirmed.

The choice to use AI is linked with political strategies. AI regulation involves existing laws, new rules, and growing domain-specific regulations. Regulation embraces

targeted rules supplemented by mechanisms to monitor and enforce variable compliance measures. Moreover, regulation denotes the effort of the state to steer the economy by compelling a set of economic controls on the behavior of private corporations. Also, AI governance involves information systems, governance and politics which means integrating policies, strategies, and mechanisms that empower AI innovation and development and constrain its diffusion through mechanisms such as regulation. Moreover, AI governance interlinks with the formulation of new rules for international interaction and engagement in areas of AI development and diffusion. Likewise, governments utilize mechanisms affecting platform behavior, which directly and indirectly influence AI governance and innovation. It seems that rules and legislation refer to areas such as platform interoperability, software accessibility, and data sharing. Correspondingly, AI presents supreme transparency, accountability, and integrity which means that via advanced analytics and predictive modeling, AI systems identify impending governance risks, fraud, and conflicts of interest and so tolerating proactive interventions and advancing compliance. Thus, by automating compliance supervising and reporting, AI advances regulatory obedience while lessening the administrative burden on governance, stimulating efficiency and accountability across institutions and corporations[57].

Sovereignty marks the unlimited power of a parliament and a state via lawmaking control sovereignty by having jurisdiction to deal with all disputes taken place in state's conventional and digital sovereignty. Likewise, Pavlos Eleftheriadis[58] argues that "Sovereignty is here part of a constitutional philosophy of democratic representation and remains a central category of modern constitutional theory, a bedrock principle."

It is worth noting that the law is grounded on the power of a state to legislate which means that law and sovereignty are functioning in tandem. On the other hand, Pavlos Eleftheriadis[59] argues "that law and sovereignty are actually incompatible. Where there is law there is no sovereignty, and where there is sovereignty there is no law." Moreover, Jacobs[60] argues that sovereignty 'is no longer a viable concept' in today's political and juridical circumstances. International law has defined sovereignty and national law clarifies the states jurisdiction to deal with all territorial disputes. It has to

be taken into account that law cannot exist on the vacuum and even a global law implies a territory that of the globe which means that sovereignty is bordered by law denoting that the law applies to the particular sovereignty. Hence, vague and very controversial claims concerning sovereignty and law do not promote the rule of law but allow unspecified powers to get authority in order to exploit the globe and so unsound arguments made in order to complicate the legal argumentation are hot air because the majesty lies on simplicity to express the big ideas promoting legality, order and society.

It could be said that a state is sovereign since it is accepted as an equal holder of 'legal personality' within the international community and so states are sovereigns when they are immune from interference by other states[61]. Sovereignty denotes an entity capable of imposing and enforcing its will[62]. To that extent, sovereignty encompasses autonomy in taking part in the global society and endorsing laws. In line, Raf Geenens[63] argues that "'sovereignty as autonomy', shows that sovereignty and the rule of law are utterly compatible… believe to be the normative core of our modern notion of sovereignty: when speaking of sovereignty, we invoke the perspective from which a political community can consciously understand itself as an autonomous agent."

Sovereignty encompasses controlling power exercised by the State on its territory, on the resources that are located in it and so digital sovereignty encompassing an endless digital sovereignty where digital transactions take part which means that a new political reality emerges[64]. Luciano Floridi[65] specifies that "Today, the fight is not over secular and spiritual power but over corporate and political power over the digita". The digital sovereignty is not replacing conventional national sovereignty but digital sovereignty overlaps national sovereignty affecting everybody and all transactions taking place via digital devices located within conventional territory.

It has to be taken into account that augmented global flows of capital, strengthened networks of social interaction, and the rise of transnational regulatory regimes are modifying the capability of national governments to regulate their economic conditions and advance their citizens' well-being. On the other hand, the consequences of

economic, technological and cultural alteration are having noteworthy effects on the activity of governing. In line, Martin Loughlin[66] argues that "sovereignty vests in the set of relations that are formed in instituting this political domain."

Who takes care of EU digital sovereignty? Can EU autonomously take care of its digital sovereignty or merely every state deal with its own digital sovereignty? Can EU exercise its sovereign powers in digital sovereignty?

In Costa v E.N.E.L[67]., the Union has been conceptualized by the Court of Justice of the European Union (CJEU) as an independent source of law and EU law displays a "legal order that has the capacity to operate as a self-referential system of norms that is both coherent and complete". Thus, European sovereignty denotes the EU as an autonomous agent which is valid when seeing the EU as legislating by adopting legislation, through the European Parliament and Council, as adjudicating by the power to engage in judicial decision-making, through the CJEU alongside national courts, as regulating by the capability to regulate, through the European Commission and regulatory agencies and as enforcing by the capacity to enforce EU law, whether through the European Commission or a national authority. On the other hand, the point that the EU legal order co-exists with the legal orders of its Member States obscures yet does not devalue EU's capacity but it denotes a limitation of competence and jurisdiction[68].

It has to be taken into account that while sovereignty is customarily conceptualized at the level of nation-states, it has been fully employed to the European context too, to the extent and degree that particular competences have been assigned to the EU by its Member States. Thus, the particular conditions needed in instigating EU sovereignty denotes the difficulty of implying EU jurisdiction on matters of EU digital sovereignty. In addition, sovereignty is not undercut by the fact that the EU can only function legitimately within the boundaries demanded by human rights, democracy and the rule of law[69]. In other words, it could be said that EU has conditional/ provisional sovereignty and consequently restricted digital sovereignty and AI sovereignty. On the other hand, nowadays there is a move towards augmenting sovereignty and so states

control cyber-sovereignty as well[70]. In line, Nathalie A. Smuha[71] specifies that "One could understand the notion of digital sovereignty as a sub-category of the EU's sovereignty".

There is an effort of states to enhance their economic digital sovereignty[72]. It seems that currently any digital sovereignty is protected via conventional sovereignty elements and not electronic measures implemented within cyberspace. Economic and normative digital sovereignty are two sides of the same coin. Moreover, EU's objective to expand its economic digital sovereignty is advantageous to the protection of the EU's values as listed in Article 2 TEU. It is characteristic that digital technologies are reforming both societies and individuals and so affecting the capacity to exercise sovereignty. Hence, the digital Services Package and the AI Package to the Data Package are perceived not only as an exercise of EU sovereignty to confirm the protection of EU values, but also as an effort to preserve and protect its sovereignty in a changing world.

French President Macron[73] announced the requirement to guarantee digital sovereignty at European level. Moreover, EU has to outline the regulatory framework that it imposes upon itself encompassing both the protection of individual liberties and the economic data. Thierry Breton[74] stresses the need for strengthening European digital sovereignty which he equated with "Europe defending its strategic interests" and "making sure that anyone who invests, operates and bids in Europe respects our rules and values."

It is pointed out that EU has to certify that EU digital Sovereignty is protected so as to form the EU digital transformation according to EU rules and values[75]. In line, Floridi[76] says that "between companies and states, the former can determine the nature and speed of change, but the latter can control the direction of change".

It has to be taken into account that the concept of European digital sovereignty encompasses the capacity of the European Union to autonomously consider EU Digital sovereignty as its sovereignty and secondly on exercising control over firstly the direction or 'destiny' of digital technology within the EU, and secondly the concrete

digital infrastructure that assists the technology. Moreover, digital sovereignty claims concern the control over digital infrastructure related with productive competencies and economic power in the digital domain. In other words, the EU's digital sovereignty not only expand in supervising digital technology and its infrastructure as such but also refer to the self-regulation of Europe's digital sovereignty through norm-setting which means that EU sets rules on digital technology and its providers through legislative, adjudicative, regulatory and enforcement actions such as binding legislation and soft law initiatives. It seems that EU market integration is a 'trading up' system, where Member States are placing more rigid rules that are in line with both the Single Market and their economic interests.

The EU AI Act launches a harmonized legal framework for AI systems that are placed on the Union market to make certain they follow existing law on fundamental rights and Union values relying on Article 114 TFEU. Moreover, the EU AI Act[77] is now in effect making certain the safe, secure, and ethical development of AI. The regulation groups AI applications grounded on risk with stricter rules for higher risk and so corporations are compelled to disclose what data their AI is being trained on, guaranteeing that it's safe to use, and going through risk assessments. Moreover, the EU AI Act categorizes AI applications into four categories such as unacceptable Risk, High Risk, Limited Risk, and Minimal Risk. Hence, High Risk systems such as financial, insurance, and employment, will be expected to undergo risk assessments, display their AI training data sets and the implicated business processes and must be continuously monitored. Furthermore, general-purpose AI (GPAI) systems must follow transparency prerequisites with documentation on the data sets used for training and confirming proper security measures.

In fact, Article 111 lays down certain rules for AI systems and GPAI models that have been already employed and put into service before the AI Act entered into force. According to Article 3(47), the AI Office stands for the Commission's purpose of contributing to AI governance along with the implementation, censoring and supervision of AI systems and GPAI models. Also, Article 70 and Recital 153 / 154 highlight that Member States play a central part in the application and

enforcement of the AI Act and so member states have to authorize at least one notifying authority and at least one market surveillance authority as national competent authorities. Hence, Member States employ any kind of public entity to accomplish the duties of the national competent authorities, in line with their particular national organizational individualities and demands. In other words, it seems that a differentiation in the applicability of AIA is ensured and so the act is not the case of a law implemented by a single jurisdiction. Furthermore, Article 56 of the AI Act delineates the Code of Practice as a means of compliance to bridge the gap between GPAI model provider obligations coming into effect and the adoption of standards. Also, AIA is compatible with regard to fundamental rights, democracy and the rule of law by requiring a set of rations on the provision and use of such systems.

It could be said that the European digital sovereignty entails the EU's capability to independently decide on its relationship with digital technology, both economically and normatively which means controlling the production of digital technologies and their principal infrastructure, along with the normative background within which such technologies activate. Can EU, alike a state, safeguard and maintain its digital sovereignty?

Digital technology and the infrastructure that empowers it is almost entirely in the hands of private companies named as 'big tech' dominating different areas of the tech industry, from artificial intelligence to cloud computing, e commerce and social networking. Also, private players influence the public area without being compelled by the obligation to act in the public interest and the requisite to be able to substantiate one's actions. In other words, decisions with normative implications are being taken by people acting in the interests of private corporations. Hence, large tech corporations are being called 'quasi-sovereign' as a result of the extent of their power[78]. Moreover, foreign entities intentionally interfere with Europe's digital sovereignty and so harmful cyber activities are directed against EU institutions and European corporations[79]. Thus, concerning these problems the question to be answered is if EU itself has got jurisdiction to defend itself alike a state.

It is characteristic that China protects its digital borders by controlling data and tech infrastructure by endorsing laws allowing direct government access to corporate data, both domestically and internationally and so adopting control of 'data-trafficking affecting not only individuals but also corporations whose data is being 'trafficked' which means that China is implementing its own digital sovereignty to amplify its control over foreign entities[80]. In line, the EU has endorsed the GDPR establishing critical safeguards against individuals' data trafficking[81] but the initiation of any legal action takes place via a member state and not the EU as a single political entity which not only makes more difficult the protection of the digital EU sovereignty but also even the conventional EU sovereignty. In addition, the global intensification in authoritarian movements makes it possible that conflicts in value-systems will jeopardize Europe's digital sovereignty[82].

It is worth mentioning here that several EU Member States have taken actions that destabilized human rights protections, deteriorated the democratic process and reduced the application of the rule of law which means that not only the EU's conventional sovereignty faces an imperative threat stemming from within the EU legal order but also the EU's digital sovereignty taking into account the expansion of digital trade. Thus, it is revealed the need for transforming current EU model into the United State of Europe (USE) which means EU is becoming a single political actor with its own jurisdiction to act and protect its own sovereignty directly alike a state.

While harms such as the risk of bias and discrimination, privacy infringements, and the erosion of the rule of law arise from the universal use of automated decision-making systems, particularly in the public sphere, the EU is urging Member States to digitalize and automate its public services. To that extent, the EU's capability to independently decide its digital course risks being weakened if it cannot be guaranteed that Member States actually abide by its digital policies. Additionally, provided the mutual trust that strengthens the EU legal system, all Member States are negatively influenced when one Member State does not enforce its commitments under EU law and so damaging the EU's external position and in case of digital matters disintegrates its unity which means that success of EU regarding the formation of the EU digital sovereignty and

implementation of digital policies to succeed demands the capacity of EU to act as a single political entity.

It has to be taken into account that if EU digital regulations are deficient, incomplete or ineffective, or if Member States fail to duly employ them, the role of digital technology in European society will not advance which means that effectiveness of EU model not having an independent political form depends on the good will of the member states which define firstly their national cyberspace sovereignty upon which get jurisdiction. In reality, through inadequate digital governance, the EU will undercut its own digital sovereignty and so the EU has to embrace robust legislative initiatives capable of steering digital technology in the direction that assures their compatibility with human rights, democracy and the rule of law[83] and implemented harmonically by all member states.

It is characteristic that AI systems are enforcing EU law, by 'translating' legal rules to code and so facilitating algorithmic regulation. With no an appropriate AI governance mechanism, it will not be possible to substantiate whether that translation arisen in a way matching with EU law. It seems that authoritarian governments are utilizing AI systems aiming to implement social control and so posing threats to basic freedoms and the rule of law. A result of the drift toward greater digital sovereignty forces states to look for critical control of digital components such as control over the international flow of citizens' data which means that the emergence of cyber state sovereignty has threaten existing forms of interconnectivity, initiating fragmentation of high technology markets to varying degrees and so retrenching back into the nation state.

The EU AI Act establishes a horizontal set of rules for developing and using AI-driven products, services, and systems within the EU. Moreover, the EU Digital Markets Act (DMA) confirms that digital platforms that possess so-called gatekeeper functions, in their access to and control of large consumer data, do not misuse their data monopolies to generate unequal market conditions and so augmenting innovation, growth, and competitiveness. Also, the EU Digital Services Act (DSA) gives consumers more control over what they see online and so better information. Additionally, the new rules protect

users not only from illegal content, but also blocking harmful content, such as political or health-related misinformation[84]. Hence, DSA imposes obligations on all online marketplaces to categorize traders offering products or services and so platforms must make efforts to make certain that the information delivered to them by the traders is truthful and complete. To that extent, AI systems allow platforms to check and control activities on them more competently. There is an accountability disparity and diffusion of responsibility where many entities are involved in a transaction.

It could be said that EU digital sovereignty signifies Europe's capability to act independently in the digital world and so EU policy-makers are inventing rations to adjust EU industrial and technological capability to the competitive environment. Also, EU policy-makers design policies to improve EU's digital strategic autonomy. It is worth noting that EU digital sovereignty and strategic autonomy generate strains between policy considerations of fundamental rights, free market principles and geopolitical concerns due to the inconsistency between the EU's considerable economic and regulatory power in digital matters and its limited mandate and capabilities in foreign policy. Hence, digital sovereignty has inherent tensions with the EU's normative power in digital issues leading to a strategic disharmony due to the functioning of the present EU model not being a federation and so EU a single political entity but its performance depends on the transferred capabilities by Member states[85].

It is distinctive that sovereignty and autonomy denote the EU economic competitiveness in the global data economy underlining both the risks and the opportunities for the EU economy and so the EU's geopolitical position is defined within and beyond cyberspace and digital issues which means that cyberspace empowers the geopolitical position of States and EU has to follow. In other words, strategic geopolitical competition has become the new principle in the digital sphere, which, in Europe, has resulted in a strategic vacuum.[86] Additionally, states are having trouble featuring the role of cyberspace by disagreeing about the applicability and boundaries of international legal principles, such as sovereignty, in cyberspace[87]. Likewise, states are undecided about the responsibility and task of large tech corporations that are

almost “quasi-sovereign” in their processes handling vast authority as they shape society’s information and performing.

It is worth noting that digital sovereignty and strategic autonomy are forcing EU to deal with digital and cybersecurity policies and so considering the current geopolitical position of EU. Hence, cyberspace, AI and digital technologies as rather unexplored territories for strategic competition driving relevant policies steadily in a geopolitical route which means that the EU has to invest in new technologies and markets, facilitate and organize intra-EU cooperation by endorsing legal frameworks. On the other hand, Zekos considers that the most important matter is its transformation into the USE in order to be able acting as a single entity and not being dependent on the national policies of the member states and their reliability. Can EU in its current form become a global player and so achieving geostrategic supremacy? By and large, the EU has to affirm itself as a geostrategic power via its transformation into a federation (USE) and the tendency for enlarging the current EU encompasses more malfunctions than leading to a more effective political scheme.

Nonetheless, as a result of the limited competence of the EU in foreign affairs, and exceedingly protected member state prerogatives when it comes to national security, unity and determination are missing at the EU level. The strength of the EU as a global player is greatly affected by its legal form and the legal basis of the policies it endorses. To that extent, Dennis Broeders[88] et al argue that “In the geopolitical domain, the EU has traditionally had less clout… the EU’s lack of a clear competence in geostrategic matters makes it very hard for member states to agree on joint strategic positions.” Hence, the alteration of the current EU model into USE is the solution.

It is worth mentioning here that all countries regard AI as a fundamental part of national security, having assimilated it into their security and defense strategies and so causing fears concerning an AI arms race and the weaponization of AI. For example, the U.S. Department of Defense unleashed a task force to explore the prospect of using AI and LLMs for military missions[89].On the other hand, due to its current model EU is far away

of implementing a common AI military policy and so wakening EU position into the globe.

Furthermore, it is worth noting here that EU is lacking formal sovereign authority but it is considered as a normative power by playing an international role as advancing a rules-based system moored in multilateral cooperation, good governance, rule of law, and human rights. Also, the presence of both competitor states and global technology corporations and platforms has advanced economic competitiveness, technological independence and preserving fundamental rights. Hence, technological innovation and progress play a central role in the process of European integration. Nevertheless, EU integration does not automatically denote that member countries have essentially 'lost' their national sovereignty which means that the sovereignty of all EU states is boosted thanks to the EU cooperation and consultation system implying more political weight[90]. Concerning the EU strategic autonomy due to technological sovereignty, EU member states guard foreign policy as a national prerogative and so the assessments of threat differ amongst member states[91]. It seems that the different assessment of EU member States regarding the EU involvement in Ukraine crisis has thrown EU into political, economic and military turmoil.

It could be said that the EU, in its present model, is difficult to become a geostrategic power due to the fact of lacking the mandate to do so and is reputationally attached to its way of running. While cyberspace progressively necessitates strategic, geopolitical thinking and action, the EU is institutionally not well equipped to produce on a strategy of strategic autonomy due to the fact that member states' individual foreign policies and national interests set a daunting hindrance to a unified security strategy[92]. Thus, the emergence of the USE is the step for not only the conventional advancement of EU into a global player but also the chance to conquer cyber-sovereignty run shortly by AAI technology and even AAI humanoids.

It has to be taken into account that global security governance is controlled by the law and governance mechanisms and security practices. Also, due to the fact that threats are not standard and there is a need of predicting, norms and concepts of global

security governance are created by soft law, legislation and technology itself initially playing the role of law in keeping legality. Rebecca Mignot-Mahdavi[93] argues that "norms produced by new sites of global security governance are particularly powerful in composing a tight legal architecture… differentiating between norms is neither possible nor helpful in global governance cosmoi where norms are interwoven, compose tight webs and strengthen one another… forms, formality, and stability are at the heart of lawmaking in sites of global security governance."

Notwithstanding the EU's many achievements and the integration process in the area of law, Europeans hardly recognize the EU's institutions as an expression of their collective autonomy. In line, Raf Geenens[94] specifies that "European citizens fail to see the EU as an expression of their collective autonomy. Despite the many material advantages offered by the EU, citizens simply cannot recognize it as a collectively acting agent of which they are part" and so denoting that the current EU model is not appropriate in designating EU as a global player.

It is characteristic that member states have assigned extensive competences such legislative, executive and judicial to EU institutions but the assigned competences are not alike that of the federal level of a federal state due to the fact that the source of EU competences lies in the founding treaties which means that EU powers are derivative since member states, which hold exclusive power to change the treaties, are staying rulers of the treaties. Moreover, the EU is an entity formed under international law and the uncertainty over its status has stayed a principal source of dispute which means that EU cannot control digital sovereignty by having direct jurisdiction to deal with disputes on cyberspace affecting directly EU people and so member states have to tackle the disputes linked with their national digital sovereignty. It has to be taken into account that while national courts acknowledge the principle of the priority of EU law, they keep the power to ascertain the limits on EU competence transfers by reference to the need of preserving basic constitutional rights[95].

It is argued that the sovereign rights of member states are curtailed by virtue of 'integration through law' due to the fact that a continuing European integration takes

place but in fact, member states keep jurisdiction to deal with matters affecting their citizens either by conventional transactions or digital transactions. Hence, EU has to develop to the level of State in order to gain and manage EU digital sovereignty[96].

In fact, the digital single market strategy contains priorities such as advancing access to digital goods and services, an environment where digital networks and services flourish by steering growth. Nonetheless, digital transformation by encompassing the dissemination of data compromises the traditional foundations of sovereignty and jurisdiction by magnifying national sovereignty and jurisdiction via the digital expansion into unterritorial dimension which on the other hand, it can be contacted via devices located within the conventional national territory. To that extent, the emergence of digital sovereignty demands the existence of independent state capable of having jurisdiction in defending the digital territory which means that regardless of EU being a regulatory actor in the field of digital technologies, its current form does not allow the functioning as a state and so having jurisdiction on the EU digital sovereignty.

On the one hand, in US corporations remain in control of AI and industrial development and governance-related criteria[97]. While the United States takes a laissez-faire approach to regulating artificial intelligence, new industrial policy initiatives are strengthening certain aspects of the AI supply chain. Moreover, the CHIPS and Science Act[98] marks a shift in U.S. industrial policy in preserving U.S. technological leadership in the face of fast-growing competition from China. The CHIPS Act is generating a robust semiconductor ecosystem by backing multiple high-volume advanced packaging capabilities, increased production of semiconductors. Also, CHIPS manufacturing funds are going towards corporations building the semiconductors that are needed to various industries such as aerospace and defense industries.

On the other hand, China's line to AI legislation is built on central government guidance and so China's regulation of algorithms goes far beyond the digital space by prescribing what type of behavior China's central government deems constructive or not in society. Also, Chinese regulations put the responsibility on private corporations to restrain, ban, or promote certain categories of content[99]. Likewise, China's central government has

intensified private partnerships with China's leading technology corporations. Artificial intelligence is considered as the device of transforming China by keeping a balance between social control and innovation. Thus, it seems that China, along with other States, will utilize even AAI humanoids for the good of China. Larsen[100] specifies that "Control over strategic resources, such as data, software, and hardware has become paramount to decisionmakers in the United States, the European Union, and China, resulting in a neo-mercantilist-like approach to governance of the digital space." Unquestionably, AI revolutionizes continuously the globe by generating values on digital trade and AI digital Sovereignty.

It is worth noting here that for the EU, digital sovereignty requires technological autonomy, individual self-determination, and regulatory power in increasing dependence on platform-based services provided by non-European corporations. Moreover, for the United States, a comparative industrial advantage in technological development is maintained along with the emergence of China as a global power[101]. In addition, for Russian Federation, digital sovereignty denotes "information security[102]", while for developing countries it is linked to digital colonialism. Also, for China, international competition vis-à-vis the United States involves controlling information unrests, restrict platform power, and protect data circulating in digital sovereignty[103].

Regarding AI governance, the EU encounters a challenge due to state and corporate rivalry alongside the materialization of a complex web of regulatory regimes. Regardless of the EU's effort for single technological sovereignty, the EU faces challenges as a consequence of its limited digital industry and its low investments linked with those of US, Russia, Japan and China.

It has to be taken into account that AI power is turned to be a technological arms races and so fighting for economic influence among states and corporations which means that AI will add in increasing geopolitical power[104] in a new arms race transforming AI as a key strategic enabler for global, national and European security. In other words, it could be argued that AI is a device of power projection and economic competence that will shape politics[105].

It is worth noting that the EU looks for its technological sovereignty by wanting to achieve strategic leadership in this sector regarding that AI is human-centric[106]. To that extent, the AI Act is introducing a horizontal, and risk-based regulation of AI systems in use and so the EU is targeting a role as a normative power in the field of AI governance. Also, in the global race for AI supremacy, all countries are trying to secure their technological power and leading position.

It has to be taken into consideration that EU is behind other countries on the financing front. Taking into account that in order to compete on the global arena, startups need considerable financial backing, there is a need to join high-tech ecosystems across Europe so as to turn innovative data from the lab to the market and into global commercial triumph. Furthermore, it is worth mentioning here that while the EU has made steps in improving AI governance via the AI Act, the union's impact on the global stage remains limited paralleled with that of US, Russia, Japan and China. Furthermore, the absence of a unified tactic among EU member states impedes EU's aptitude to speak with a consistent voice on the global stage. To that extent, all these obstacles will be overtaken by transforming the EU into USE which means a new political entity with a common voice in the global arena.

It is characteristic that the geopolitics of AI discloses a rivalry among the United States and China involved in a race to ascertain supremacy in AI capabilities which in fact has sweeping consequences for EU's economic stand, military power, and global impact[107]. To that extent, Raluca Csernatoni[108] argues that "EU policymakers should carefully consider the complex relationship between the act and other EU legislation while identifying and addressing potential loopholes that may not be readily apparent and may be subtly exploited."

It is worth noting that France has disputed that particular clauses in the AI Act impede national AI innovations and so setting obstacles for European AI startups such as France's Mistral AI, LightOn, and Hugging Face[109]. Thus, the EU model[110] seems to reveal its weakness to run as a single political entity like US or China and so revealing

the need for an immediate transformation into the USE where laws will be implemented under a single understanding generating a harmonious advancement of AI.

It is typical that centralized legislation encourages political participation and efficiency, diminishing forum shopping, and fostering policy coordination permitting effective management to drop costs[111]. Further, like EU AI Act, a centralized body of laws eliminates conflicting and overlapping laws and so removing forum shopping perpetuated by fragmented legislation, where corporations can choose which states to participate in. Lastly, coordination between member states in the EU with a centralized legislative body is achieved by addressing policy issues arising from the repetitively changing landscape of AI and so the EU AI Act is the first step towards horizontal, centralized AI legislation. On the other hand, the current model of EU generates problems concerning the implementation of central laws and so the transformation of EU into USE will allow the standardization in the applicability of laws.

8. Conclusions

The digital society epitomizes a new society governed via the use of information and communication technologies and so a digital society is a networked information society with new values and needs[112] It is characteristic that digital data's distinctive relationship with territory is demonstrated by cross-border data flows The growth of data flows and widespread digital transformation illustrate the digital territorial domain where borderless networks are challenging the conventional territorial order of states. Moreover, the collection, control, and use of data transform political, economic, and social power, which is considered as a threat to a sovereign state but, in fact, states have already taken actions in controlling cyber-sovereignty and AI digital sovereignty. Additionally, the territorialization of cyberspace, cyber-sovereignty and AI digital sovereignty bring forward another dimension in exercising jurisdiction upon transactions taken part in digital domain. It seems that currently territorialization can be achieved by states via electronic and AI technology which is located within their

conventional territory and getting jurisdiction according to various conventional criteria.

It seems that the legal nature of the EU and the question of the transfers of powers from the member states to the EU generate problems in the emergence of the EU digital sovereignty. EU digital sovereignty stipulates/ requires EU's capability to act independently in the digital world in terms of jurisdiction, defensive mechanisms and offensive means.

Taking into account that the principle of territoriality is the central basis for the assertion of jurisdiction in international law,[113] jurisdiction is attributed to the state in all matters that are within its territorial sovereignty[114] which means that EU has to be considered as a state, a sole political entity, in order to get autonomous jurisdiction and so gaining EU digital sovereignty.

Can the idiotypic model of EU allow autonomous jurisdiction exercised to an autonomous EU conventional and digital sovereignty? Jurisdiction is certainly territorial which means that jurisdiction is exercised on defined bordered territory and so it seems that due to EU model exercising jurisdiction in the sense of state jurisdiction is not applicable in the case of EU prohibiting the defense of autonomous EU digital sovereignty but member states have jurisdiction upon their own digital sovereignty. Especially, in the cases of Schrems I and Schrems II, the CJEU highlights the supreme power of national data protection authorities regarding the European Commission, on the one hand, and in relation to states outside the EU, on the other[115].

NOTES

- BS(ECON), JD, LLM, PHD (LAW) PHD (ECON) International Hellenic University, Serres - Macedonia, Hellas zekosg@ihu.gr

[1] Crane, A./Matten, D. (2007): Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization, 2nd, Oxford University Press: Oxford.

[2] Reno v. ACLU, 521 U.S. 844.

[3] Shoshana Zuboff, The Age Of Surveillance Capitalism: The Fight For A Human Future At The New Frontier Of Power 104 (2019) ("lawlessness" has been instrumental to the rise of surveillance capitalism).

[4] *G Zekos, Cyber-Territory And Jurisdiction* Of Nations, 2012 *Journal of Internet Law*, Number 12/3, G. Zekos, Globalisation and States' Cyber-Territory', [2011] 5 Web JCLI.

[5] Zekos, G. (1999), "Internet or electronic technology: a threat to state sovereignty", JILT,: www.law.warwick.ac.uk/jilt/99-3/zekos.html , G Zekos, Demolishing State's sole power over Sovereignty & Territory via Electronic Technology & Cyberspace, 2013 Journal of Internet Law, Volume 17 Number 5 November 2013 27-41 Aspen Publications- Wolters Kluwer.

[6] OECD, WTO, IMF (2020), Handbook on Measuring Digital Trade, OECD Publishing. Ismail, Y. (2023), The Evolving Context and Dynamics of the WTO Joint Initiative on E-commerce, https://www.iisd.org/system/files/2023-04/wto-joint-initiative-e-commerce-fifth-year-stocktakeen.pdf. Jaax, A., S. Miroudot and E. van Lieshout (2023), "Deglobalisation? The reorganisation of global value chains in a changing world", OECD Trade Policy Papers, No. 272, OECD Publishing, Paris, https://doi.org/10.1787/b15b74fe-en. Herman, P. and S. Oliver (2022), "Trade, Policy and Economic Development in the digital economy", USITC Economics Working Paper. APEC Committee on Trade and Investment, Economic Impact of Adopting Digital Trade Rules: Evidence from APEC member Economies, 2023 https://www.apec.org/

[7] Cheng, Jing, and Jinghan Zeng. 2022. Shaping AI's Future? China in Global AI Governance. Journal of Contemporary China 1–17. https://doi.org/10.1080/10670564.2022.2107391.

[8] Neil Weinstock Netanel, Cyberspace Self – Governance: A Skeptical View from Liberal Democratic Theory 88 Calif. L.Rev. 395 (2000).

[9] *In re* C.K.G., 173 S.W.3d 714, 730-32.

[10] *Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 167.

[11] *Commonwealth v. 141 Internet Domain Names*, No. 08-CI-1409.

[12] Sun Microsystems, Inc. v. Microsoft Corp., 240 F. Supp 2d 460.

[13] Hughes v. Alexandria Scrap Corp. 426 U.S. 794, Reeves, Inc. v. Stake 447 U.S. 429

[14] Reno v. ACLU, 521 U.S. 844

[15] *American Banana Co v United Fruit Co* 213 US 347

[16] Shulamit Almog, *From Sterne and Borges to Lost Storytellers: Cyberspace, Narrative, and Law,* 13 Fordham Intell. Prop. Media & Ent. L.J. 1, 3 (2002)

[17] Paul Schiff Berman, *The Globalization of Jurisdiction,* 151 U. PA. L. REV. 311, 321-22 (2002)

[18] Peter J. Spiro, "Globalization, International Law, and the Academy," 32 *N.Y.U.J. Int'l L. & Pol.* 567, 568 & n.2 (2000) (noting that the term " 'post national' has crept into other disciplines," but that international law scholars have been slow to pick up the term, having "only recently caught on to 'globalization' ").

[19] A. Bianchi, "Jurisdictional Rules in Customary International Law," at 87 in K.M. Meessen, (ed.), Extraterritorial Jurisdiction in Theory and Practice, The Hague: Kluwer Law International (1996).

[20] H.L. Buxbaum, "National Jurisdiction and Global Business Networks," 17 *Ind. J. Global Legal Stud.* 165, 167 (2010) (arguing that "a global problem can be recast in local terms, in order to take advantage of local political or social resources" and suggesting use of the concept of scale to understand this analytically).

[21] Todd David Peterson, Categorical Confusion in Personal Jurisdiction Law, 76 Wash. & Lee L. Rev. 655, 680–82 (2019)

[22] Ford Motor Co. v. Montana Eighth Judicial District Court. 141 S. Ct. 1017 (2021)

[23] Burnham v. Superior Ct. of California, 495 U.S. 604 (1990).

[24] Goodyear v. Brown, 564 U.S. 915 (2011). BNSF Railway Co. v. Tyrrell, 581 U.S. 402 (2017).

[25] Mallory v. Norfolk S. Ry. Co., 143 S. Ct. 2028 (2023).

[26] *eDirectives: Guide to European Union Law on ECommerce- Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection*, Kluwer Law International, The Hague - London - New York, 2002, *EU Information Society Guide*, The EU Committee of the American Chamber of Commerce in Belgium, Brussels, 1996 Arno R. Rodder and Henrik W.K. Kaspersen (eds.).

[27] International Law Commission (ILC), 'Report on the Work of its Fifty-Eighth Session' (1 May-9 June and 3 July-11 August 2006) UN Doc A/61/10.

[28] Bank Mellat v. Helleniniki Tecchniki S.A. [1984] Q.B. 291. (the concept of arbitral procedures floating in the transnational firmament, unconnected with any municipal system of law)

[29] James Crawford, The creation of states in international law 26-27 (1979)

[30] Stephen D. Krasner, Sovereignty: Organized Hypocrisy (1999).

[31] Gilson, Bernard, *The Conceptual System of Sovereign Equality*. Leuven: Peeters, 1984.

[32] Masilamani, N., & Anup Kurvilla John., *"The future of State Sovereignty: Emerging Concerns in the Internet Era"* (The student Advocate, Volume 13, 2001).

[33] *Gregory v. Ashcroft* 501 U.S. 452, 460 (1991)

[34] Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 Fed. Comm. L.J. 117, 129–42 (1997).

[35] Nixon v. Missouri Municipal League. 541 U.S. 125

[36] David R. Johnson & David G. Post, Law and Borders: The Rise of Law in Cyberspace, 48 Stan. L.Rev. 1367 (1996).

[37] G. Zekos, "State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction," *International Journal of Law and Information Technology"* (Oxford University Press 2005), *available at* http://ijlit.oxfordjournals.org/ content/15/1/1.short.

[38] Simmons, B. and Hulvey, R. (2023), Cyber Borders: Exercising State Sovereignty Online. Temple Law Review 95, pp.617–640, https://scholarship.law.upenn.edu/faculty_scholarship/3158

[39] Yassin Abdalla Abdelkarim, A literature review of the evolution of sovereignty and borders concepts in cyberspace, International Cybersecurity Law Review (2024) 5:365–372 p369

[40] Zekos GI (2022) Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society. Springer Nature Switzerland https://doi.org/10.1007/978-3-030-94736-1

[41] Montevideo Convention on the Rights and Duties of States, art. 1, Dec. 26, 1933, 49 Stat. 3097, T.S. 881, https://www.hlrn.org/img/documents/Montevideo_Convention.pdf ("The state as a person of international law should possess the following qualifications: a) a permanent population; b) a defined territory; c) government; and d) capacity to enter into relations with the other states."

[42] Beth A. Simmons & Hein E. Goemans, Built on Borders: Tensions with the Institution Liberalism (Thought It) Left Behind, 75 INT'L ORG. 387, 387–410 (2021);

[43] Beth A. Simmons & Michael R. Kenwick, Border Orientation in a Globalizing World, 66 AM.J. POL. SCI. 853 (2022).

[44] Montevideo Convention on the Rights and Duties of States, art. 1, Dec. 26, 1933, 49 Stat. 3097, T.S. 881, https://www.hlrn.org/img/documents/Montevideo_Convention.pdf ("The state as a person of international law should possess the following qualifications: a) a permanent population; b) a defined territory; c) government; and d) capacity to enter into relations with the other states.").

[45] Beth A. Simmons & Hein E. Goemans, Built on Borders: Tensions with the Institution Liberalism (Thought It) Left Behind, 75 Int'l Org. 387, 387–410 (2021);

[46] Beth A. Simmons & Rachel A. Hulvey, Cyberborders: Exercising State Sovereignty Online , 2023 Temple Law Review Vol. 95/617 P639

[47] Adam Satariano & Valerie Hopkins, Russia, Blocked From the Global Internet, Plunges Into Digital Isolation, N.Y. TIMES (Mar. 7, 2022), https://www.nytimes.com/2022/03/07/technology/russia-ukraineinternet-isolation.html Yingdan Lu, Jack Schaefer, Kunwoo Park, Jungseock Joo & Jennifer Pan, How Information Flows from the World to China, 2022 Int'l J. Press/Pol. Onlinefirst 1, https://doi.org/10.1177/194016122211174

[48] T.R. Reid, The United States of Europe: The New Superpower and the End of American Supremacy, 2005 by Penguin Books

[49] G Zekos, The United States of Europe The Global Player, 2019 Nova Science Publications New York USA. www.novapublishers.com G Zekos, The United States of Europe in place of the European Union, 2017 Nova Science Publications New York USA. www.novapublishers.com

[50] G Zekos, How Will Ai Influence Politics? Chance Or Danger For Democracy? Cicero Foundation Great Debate Paper No. 22/03

[51] Moerrel, L., & Timmers, P. (2021). Reflections on digital sovereignty EU. EU Cyber Direct, Research in Focus Series, 2021, 33 Digital sovereignty is defined as "the capabilities and capacities to decide and act autonomously on essential aspects of the longer-term future in the economy, society and democracy". Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy & Technology, 33, 369–378 Digital sovereignty is specified as "the control of data, software (e.g. AI), standards and protocols (e.g. 5G, domain names), processes (e.g. cloud computing), hardware (e.g. mobile phones), services (e.g. social media, e-commerce), and infrastructures (e.g. cables, satellites, smart cities), in short, for the control of the digital"

[52] Tsagouring, N., & Buchan, R. Can we have sovereignty without borders? (2015). Research handbook on international law and cyberspace (p. 672). Edward Elgar Publishing.

[53] Beth A. Simmons & Hein E. Goemans, Built on Borders: Tensions with the Institution Liberalism (Thought It) Left Behind, 75 INT'L ORG. 387, 387–410 (2021); Jordan Branch, Mapping the Sovereign State: Technology, Authority, and Systemic Change, 65 INT'L ORG. 1, 1–36 (2011).

[54] Schmitt, Lewin. 2022. Mapping Global AI Governance: A Nascent Regime in a Fragmented Landscape. AI and Ethics 2 (2): 303–314. https://doi.org/10.1007/s43681-021-00083-y.

[55] Charles S. Maier, Once Within Borders: Territories Of Power, Wealth, And Belonging Since 1500, at 16, 65, 67 (2016). Michael Grothaus, Get Ready for the "Splinternet": The Web Might Not be the Worldwide Much Longer, FAST COMPANY (Sept. 7, 2018), https://www.fastcompany.com/

[56] Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Platforms and infrastructures in the digital age. Information Systems Research, 29(2), 381–400. https://doi.org/10.1287/isre.2018.0794

[57] Sigrist, F., & Leuenberger, N. (2023). Machine learning for corporate default risk: Multi-period prediction, frailty correlation, loan portfolios, and tail probabilities. European Journal of Operational Research, 305(3), 1390-1406.

[58] Pavlos Eleftheriadis, Law And Sovereignty, Law and Philosophy (2010) 29:535–569 p 538

[59] Pavlos Eleftheriadis, Law And sovereignty, Law and Philosophy (2010) 29:535–569 p 535

[60] Francis Jacobs, The Sovereignty of Law: The European Way (Cambridge: Cambridge University Press, 2007), p. 5.

[61] Jean Cohen, Globalization and Sovereignty. Rethinking Legality, Legitimacy, and Constitutionalism (Cambridge: Cambridge University Press, 2012)

[62] Thomas D. Grant, 'Defining Statehood: The Montevideo Convention and its Discontents', Columbia Journal of Transnational Law 37 (1999): pp. 403 457.

[63] Raf Geenens, Sovereignty As Autonomy, Law and Philosophy (2017) 36: 495–524 p495

[64] Damian Chalmers and Luis Borroso, 'What Van Genden Loos stands for,' International Journal of Constitutional Law 12 (2014): 105-34 (accepting the 'police logic' of EU law but following Agamben's argument that the essential element of sovereignty is the power over life, arguing that this instrumentalization of law does not erode 'sovereignty').

[65] Luciano Floridi, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, Philosophy & Technology (2020) 33: 369-378 p 377.

[66] Martin Loughlin, The Erosion of Sovereignty, 2016Netherlands Journal of Legal Philosophy 57 (45) 2 p 59

[67] Case 6/64, Judgment of the Court of 15 July 1964, Flaminio Costa v E.N.E.L., ECLI:EU:C:1964:66

[68] Koen Lenaerts, José A Gutiérrez-Fons and Stanislas Adam, 'Exploring the Autonomy of the European Union Legal Order' (2021) 81 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht / Heidelberg Journal of International Law 47, 48.

[69] Raf Geenens, 'Sovereignty as Autonomy' (2017) 36 Law and Philosophy 495.

[70] Roxana Vatanparast, 'Data Governance and the Elasticity of Sovereignty' (2020) 46 Brooklyn Journal of International Law 1, 3.

[71] Nathalie A. Smuha Digital Sovereignty In The European Union: Five Challenges From A Normative Perspective Working paper - ERA Conference Proceedings https://ssrn.com/abstract=4501591 P3

[72] Dennis Broeders, Fabio Cristiano and Monica Kaminska, 'In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions' [2023] Journal of Common Market Studies 1, 5.

[73]Emmanuel Macron, 'Discours du Président Emmanuel Macron sur la stratégie de défense et de dissuasion devant les stagiaires de la 27ème promotion de de guerre' (7 February 2020) https://www.elysee.fr/emmanuelmacron/2020/02/07/discours-du-president-emmanuel-macron-sur-la-strategie-de-defense-etde-dissuasion-devant-les-stagiaires-de-la-27eme-promotion-de-lecole-de-guerre

[74] Thierry Breton, 'Speech by Commissioner Thierry Breton at Hannover Messe' (Hannover Messe Digital Days, 20 July 2020) <https://ec.europa.eu/commission/presscorner/detail/es/speech_20_1362>

[75] European Commission, '2030 Digital Compass: The European Way for the Digital Decade' (2021) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions COM/2021/118 final.

[76] Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU' (2020) 33 Philosophy & Technology 369, 369

[77] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[78] Natasha Lomas, 'Report Reveals How Big Tech Lobbied to Weaken EU Rules' TechCrunch (22 April 2022)

https://techcrunch.com/2022/04/22/google-facebook-apple-eu-lobbying-report/

[79] Jean-François Bobier and others, 'Can Europe Create Its Own Deep-Tech Giants?' (Boston Consulting Group 2022) https://www.bcg.com/publications/2022/how-can-europe-builddeep-tech-leaders Stuart Lau, 'Europe Joins US to Condemn Cyberattacks from China' POLITICO (19 July 2021 <https://www.politico.eu/article/europe-us-condemnation-china-state-sponsoredcyberattacks/>

[80] Aynne Kokas, Trafficking Data: How China Is Winning the Battle for Digital Sovereignty (Oxford University Press 2022)

[81] Zuzanna Gulczyńska, 'A Certain Standard of Protection for International Transfers of Personal Data under the GDPR' (2021) 11 International Data Privacy Law 360. Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 79I , 21 March 2019, p 1–14). Jakob Hanke and Barbara Moens, 'EU Looks to Ban Companies from Making Sensitive Tech in China' POLITICO (20 June 2023) https://www.politico.eu/article/eu-ban-companiesmake-sensitive-tech-china/

[82] Freedom House, 'Freedom in the World 2022: The Global Expansion of Authoritarian Rule' (2022) https://freedomhouse.org/sites/default/files/202202/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

[83] Robert Spano, 'The Rule of Law as the Lodestar of the European Convention on Human Rights: The Strasbourg Court and the Independence of the Judiciary' (2021) 27 European Law Journal 211.

[84] Madiega Tambiama, 'Digital Sovereignty for Europe' (European Parliamentary Research Service 2020) EPRS Ideas Paper.

[85] Dennis Broeders, Fabio Cristiano And Monica Kaminska, In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions, JCMS 2023 Volume 61. Number 5. pp. 1261–1280

[86] Liebetrau, T. (2022) 'Cyber Conflict Short of War: A European Strategic Vacuum'. European Security, Vol. 31, pp. 497–516. https://doi.org/10.1080/09662839.2022.2031991

[87] Delerue, F. (2020) Cyber Operations and International Law (Cambridge (UK): Cambridge University Press).

[88] Dennis Broeders, Fabio Cristiano And Monica Kaminska, In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions, JCMS 2023 Volume 61. Number 5. pp. 1261–1280 p 1262

[89] Josh Luckenbaugh, "New Pentagon Task Force Exploring Generative AI," National Defense, October 25, 2023, https://www.nationaldefensemagazine.org/articles/2023/10/25/new-pentagon-task-force-exploring-generative-ai. Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., and Floridi, L. "Artificial Intelligence and the 'Good Society': the US, EU, and UK approach." Science and Engineering Ethics 24, no. 2: 505–528. https://doi.org/10.1007/s11948-017-9901-7 https://www.commerce.gov/tags/chips-and-science-act

[90] Monsees, L. and Lambach, D. (2022) 'Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity'. European Security, Vol. 31, No. 3, pp. 377–394. https://doi.org/10.1080/09662839.2022.2101883

[91] Meijer, H. and Brooks, S.G. (2021) 'Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back'. International Security, Vol. 45, No. 4, pp. 7–43. https://doi.org/10.1162/isec_a_00405

[92] Timmers, P. (2022) How Europe aims to achieve strategic autonomy for semiconductors. Brookings Institute, 22 August 2022.

[93] Rebecca Mignot-Mahdavi, The Legal Fabrique Of Global Security Governance, https://ssrn.com/abstract=4652568 p 29-30.

[94] Raf Geenens, Sovereignty As Autonomy, Law and Philosophy (2017) 36: 495–524 p519

[95] Monica Claes, The National Courts' Mandate in the European Constitution (Oxford: Hart, 2006).

[96]See Carl Schmitt, Constitutional Theory [1928] (Durham, NC: Duke University Press, 2008), (Schmitt regards the federation as serving 'the common goal of political self-preservation of all federation members'). Ivic, S., & Troitiño, D. R. (2022). Digital sovereignty and identity in the European union: A challenge for building Europe. European Studies, 9(2), 80–109. https://doi.org/10.2478/eustu_2022-0015.

[97] Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., and Floridi, L. "Artificial Intelligence and the 'Good Society': the US, EU, and UK approach." *Science and Engineering Ethics* 24, no. 2: 505–528. https://doi.org/10.1007/s11948-017-9901-7

[98] https://www.commerce.gov/tags/chips-and-science-act

[99] Huld, A. China's Sweeping Recommendation Algorithm Regulations in Effect from March 1. *China Briefing*. January 6, 2022. https://www.china-briefing.com/news/china-passes-sweeping-recommendation-algorithm-regulations-effect-march-1-2022/

[100] Larsen, B. C. (2022). Governing Artificial Intelligence: Lessons from the United States and China. Copenhagen Business School [Phd]. PhD Series No. 29.2022

[101] Metakides, George. 2022. A Crucial Decade for European Digital Sovereignty. In Perspectives on Digital Humanism, ed. Hannes Werthner, Eric Prem, Edward A. Lee, and Carlo Ghezzi, 219–226. Cham: Springer.

[102] Daucé, Françoise, and Francesca Musiani. 2021. Infrastructure-Embedded Control, Circumvention and Sovereignty in the Russian Internet: An Introduction. First Monday 26(5). ff10.5210/fm.v26i5.11685ff.

[103] Creemers, Rogier. 2020. China's Approach to Cyber Sovereignty. Berlin: Konrad Adenauer Stiftung. https://www.kas.de/en/single-title/-/content/china-s-approach-to-cyber-sovereignty.

[104] Barry Pavel et al., "AI and Geopolitics: How Might AI Affect the Rise and Fall of Nations?," RAND Corporation, November 3, 2023, https://www.rand.org/pubs/perspectives/PEA3034-1.html.

[105] Jascha Bareis and Christian Katzenbach, "Talking AI Into Being: The Narratives and Imaginaries of National AI Strategies and Their Performative Politics," Science, Technology, & Human Values 47, no. 5 (2022): 855–881, https://doi.org/10.1177/01622439211030007

[106] A European Approach to Artificial Intelligence," European Commission, January 31, 2024, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

[107] Raluca Csernatoni, "Beyond the Hype: The EU and the AI Global 'Arms Race,'" European Leadership Network, August 21, 2019, https://carnegieeurope.eu/2019/08/21/beyond-hype-eu-and-ai-global-arms-race-pub-79734

[108] Raluca Csernatoni, Charting the Geopolitics and European Governance of Artificial Intelligence, 2024 2024 Carnegie Endowment , CarnegieEndowment.org P21

[109] Alexandre Piquard, "France Keeps Up Pressure on EU's AI Act, Despite Mounting Criticism," Le Monde, January 27, 2024, https://www.lemonde.fr/en/economy/article/2024/01/27/france-keeps-up-its-pressure-on the-eu-s-ai-act-despite-mounting-criticism_6471038_19.html.

[110] Julia Tar and Luca Bertuzzi, "AI Office Established, AI Convention's Scope Struggle," Euractiv, January 26, 2024, https://www.euractiv.com/section/digital/news/ai-office-established-ai-conventions-scope-struggle.

[111] Dane Chapman, The Ideal Approach to Artificial Intelligence Legislation: A Combination of the United States and European Union, 78 U. MIA L. Rev. 265 (2023) https://repository.law.miami.edu/umlr/vol78/iss1/8

[112] G Zekos, Political, Economic and Legal Effects of Artificial Intelligence, 2022, https://link.springer.com/book/10.1007/978-3-030-94736-1#toc G Zekos, Economics and Law of Artificial Intelligence - Finance, Economic Impacts, Risk Management and Governance, 2021 www.springer.com Zekos considers that the spiritual life of humans cannot be replicated via AAI technology. see chapter 11 G Zekos, Advanced Artificial Intelligence and Robo-Justice,2022, www.springer.com Γ. Ζέκος, Τεχνητή Νοημοσύνη & Ανταγωνισμός, 2024 https://www.sakkoulas.gr/en/editions/g-zekos-techniti-noimosyni-antagonismos-2024/ Γ. Ζέκος, Τεχνητή νοημοσύνη, μεταφορές & ευθύνη των μεταφορέων στο ελληνικό δίκαιο, 2023 https://www.sakkoulas.gr/en/editions/g-zekos-techniti-noimosyni-metafores-evthyni-ton-metaforeon-sto-elliniko-dikaio-2023/ Γ. Ζέκος, Διαδίκτυο & τεχνητή νοημοσύνη στο Ελληνικό δίκαιο, 2022 https://www.sakkoulas.gr/en/editions/g-zekos-diadiktyo-techniti-noimosyni-sto-elliniko-dikaio-2022/

[113] Ryngaert, C. (2015). Jurisdiction in International Law (2nd Edition). Oxford University Press.

[114] The case of the S.S. "LOTUS" (France v. Turkey). Judgment of 7 September 1927. PCIJ Series A—No 10. https://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf

[115] (Case C-311/18). Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems Judgment of the Court (Grand Chamber) of 16 July 2020. https://curia.europa.eu/juris/liste.jsf?num=C-311/18