Andreea DRAGOMIR
Lucian Blaga University of Sibiu, Romania

IMPLICATIONS OF DIGITIZATION ON PUBLIC SPACE

Abstract:	*The period of social distancing and the transfer of social and private activities to the digital environment can be a formative experience that, in the medium term, can lead to the development of an ethical, educational, legal, and administrative system in which digital citizenship is a basic component of interactions between individuals.* *The article develops the prerequisites for the real digitization of public space, which involves the use of electronic means so that social relations in the virtual environment are offered solutions for regulating and responding to developments in the digital domain through coherent and functional anticipation.* *The security of the digital environment and the complex risks and threats to cybersecurity implicitly impact national, European, and international public space.*
Keywords:	**Public space; digital space; digital sovereignty; digital citizenship; digital identity; digital security**
Contact details of the authors:	E-mail: andreea.dragomir@ulbsibiu.ro
Institutional affiliation of the authors:	**Lucian Blaga University, Simion Bărnuțiu Faculty of Law**
Institutions address	Calea Dumbrăvii 34, Sibiu, Romania 550324

Introduction

The phenomenon of digitization is not a current one, but concerns about the implementation of new information technologies in all areas of activity have led to a massive spread of the scope of digitization and the information society.

The digital space can be conceived of as a public space, which in turn is dominated by an ideology driven by interactions between individuals. Consequently, the digital public space is the product of interaction between individuals, a field of variable intensity, strictly dependent on the progress of the quality and quantity of the internet and digital technologies, which have practically transformed the world we live in, creating a new dimension of public space, the analysis of which is carried out mainly by J. Habermas.

We begin our analysis of the proposed topic by defining the basic term, *public space,* or public sphere[275]. Public space is an environment, which is based on political reason, a space where individuals can express themselves freely, without constraints of time, and resources, and where arguments prevail over power and status[276]. This space is created by the very interactions between individuals willing to accept that argued ideas have more power than the authority of tradition[277]. Habermas originally conceived public space as a form of mediation between the

[275]Jurgen Habermas, *Sfera publică și transformarea ei structurală*, Comunicare.ro, București, 2005
[276]Dragoș Dragoman, *Declinul democratic din România după 2007*, TehnoMedia, Sibiu, 2022, p. 38
[277]Pauline Johnson, *Habermass Search for the Public Sphere*, in ”European Journal of Social Theory”, Vol. 4, No. 2, 2001, pp. 215-236

state and civil society. However, the conditions of communication through which the opinion and will of the public of citizens are formed are reflected in social relations of inequality and domination. These characteristics of social relations are since communication processes belong to different social fields, and therefore access to public space is different, unequal, and conflictual.

The boundary between the real world and the digital world has become blurred. However, if we look at the characteristics of digital space, we will find that this space is not free for exploration and use for various reasons[278] even if the boundaries of this space are not analogically determinable. We experience socio-economic barriers regarding access, the information we consume online is increasingly mediated by algorithms, and searching depends largely on the information, data searched, and available to the public.

At the same time, existing online barriers restrict access to products and services, which means, among other things, removing barriers to online trade. This problem has been addressed by the EU Regulation 2018/302[279] which addresses the issue of unjustified discrimination about online sales based on the nationality or nationality, residence, or headquarters of customers within the internal market. Banning geo-blocking is an important element of the Digital Single Market strategy[280].

Another very important point to make is that digital space is not controlled by states alone. It is increasingly controlled by non-state entities, especially private companies. This is, of course, where we should point out that we are developing the subject within democratic states, as authoritarian states have a different attitude to access to information.

In recent decades, the level of trust in national governments has been steadily declining. Public administrative strategies to increase trust in government have focused on popularizing the benefits of government, improving services, and - perhaps most importantly - equipping individuals with the means to influence public policy and government decision-making, online applications, or e-democracy[281].

These directions are proving to be ideal since such innovations help cultivate an environment where information is accessible, people feel more connected to their governments, and citizens specialize in participating in political processes, with cooperation and assistance being the main priorities. Examples might include open-source innovations or simply Facebook groups that have brought us closer to like-minded people.

The importance of open-source information has increased as the globalization of information has expanded. A relevant experiment conducted by the US intelligence community revealed the importance of open-source information in the field of security[282]. Also, The USA Information Community established that OSINF represents the data available to the public, which could be electronic or printed and can be transmitted via television, radio, newspapers,

---

[278]Mirela Mărcut, *Spațiul digital nu e ca spațiul cosmic. Despre suveranitatea digitală*, in ”Digital”,European Union, https://digitalpolicy.ro/2021/05/22/spatiul-digital-nu-e-ca-spatiul-cosmic-despre-suveranitatea-digitala, (25.01.2023)

[279]*Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on the prevention of unjustified geo-blocking and other forms of discrimination based on nationality or nationality, domicile, or the registered office of customers in the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394* and *Directive 2009/22/EC*, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32018R0302, (26.01.2023)

[280]*Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions. A Digital Single Market Strategy for Europe*, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52015DC0192, (26.01.2023)

[281]Ibidem, p. 11

[282] Nicoleta Annemarie Munteanu, *Illegal migration approach from the perspective of open source intelligence (OSINT)*, in ”Research and Science Today”, No.2 (18)/2019, p. 104

databases, and portable media. These can be propagated to a broad audience, to a heterogeneous public specifically within mass media, but also to well-defined groups[283].

Also, worth mentioning in this category is the series of protest movements that have taken place in several countries in the Middle East and North Africa since the end of 2010 - the Arab Spring. The protests took place mainly in Arab countries where authoritarian or totalitarian regimes reigned and the existence of modern means of communication such as Facebook or Twitter facilitated the organization of the uprising, which is why the governments of several countries affected by the protests blocked access to them or even to the entire Internet. International media access in several countries has been severely restricted and reporters from several international broadcasting channels (CNN, Al Jazeera, etc.) on the ground have been threatened, detained by police, or even beaten[284].

Digital democracy is an attempt to practice the democratic system outside the confines of time, space, and other physical conditions, using information and communication technology or computer-mediated communications to replace or supplement but not exclude traditional or analog political processes. In other words, digital democratic applications are seen as alternative means of democratic participation[285].

At the EU level, digital democracy is already being implemented. Public authorities are using the Internet to facilitate an open dialogue between citizens and the government. The digital transformation element represents a novel vision in the public sector, and the adoption of this approach presents advantages such as increased efficiency, transparency, and simplification that enhance the productivity of processes to a considerable degree. Leaders of public institutions must recognize the importance of adopting new technologies, continually adapting to the evolving needs of citizens, and prioritizing the provision of quality, secure, and prompt online public services. Consequently, the involvement of citizens in the policy-making process is bolstered, the authorities' capacity to react swiftly and accurately to the public's concerns is augmented, and the expenses incurred by the government are curtailed.

In Romania, the Authority for the Digitization of Romania (ADR)[286] is the structure with legal personality within the Ministry of Research, Innovation, and Digitization, whose role is to carry out and coordinate the implementation of strategies and public policies in the field of digital transformation and information society.

E-government is a complex interaction between society and technology. Amidst the COVID-19 pandemic, digital technologies have facilitated the interaction between governments and their populace, as well as continued the provision of services online. In numerous nations, the digital government has taken on an even more critical role, serving as an essential component of communication, governance, and cooperation between policymakers and society. However, apprehensions surrounding privacy and the dissemination of false information have mounted. Evidence of successful implementation of eGovernment can be observed in the US, Canada, the

---

[9] In 1995 The Aspin-Brown Commission, formally titled The Commission on the Roles and Capabilities of the United States Intelligence Community was charged with reviewing the entire US international community, and the experiment suggested naming open sources against secret sources.

[284] *EU's response to the "Arab Spring": The State-of-Play after Two Years, official EU document*, 8 February 2013, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/135292.pdf., (04.04.2023)

[285] Europe Direct Information Centre Timisoara, *Digital Citizen's Guide*, 2018, p. 13, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europedirect-tm.ro/wp-content/uploads/2018/12/Ghidul_cetateanului_digital_2018.pdf, (04.04.2023)

[286] ADR, *Transformarea digitală a instituțiilor publice*, https://www.adr.gov.ro/transformarea-digitala-a-institutiilor-publice/, (04.04.2023)

UK, Estonia, as well as other northern European countries that have reached an advanced stage of eGovernment.

In the context of the public sector's use of information and communication technologies to improve access to information and services provided by public administration authorities through fast and efficient service to the citizen, the citizens have an imperative role to play in correctly assessing the efficiency and security of this digitally enabled public sector.

Thus, the citizen, accessing the facilities of the government-citizen partnership (transparent administration for citizens, improved services in terms of quality, convenience, cost, and active involvement of citizens in decisions and actions in the public sector) must abide by a code of ethics for the use of artificial intelligence both in the judiciary and in the administrative system[287].

With the transfer of specific administrative and judicial activities to the virtual environment, the transfer of fundamental rights of individuals, as laid down in the European Convention on Human Rights (ECHR) and the Convention on the Protection of Personal Data, must also take place. Under these circumstances, the digital environment must:

- design and implement artificial intelligence tools and related services compatible with fundamental rights;
- specifically prevent the development or intensification of any discrimination between individuals or groups of individuals;
- process documents and data, using certified sources and intangible data, developed in a multidisciplinary manner, in a secure technological environment;
- ensure that users are informed actors and make informed decisions[288].

With a *Code of Ethics on the Use of Artificial Intelligence*[289] and an *Internet Education (Literacy) Manual*[290] published by the Council of Europe, we can also talk conceptually about digital citizenship.

Digital citizenship can be defined as engaging citizens in appropriate and responsible behavior when using technology. Digital citizenship specifically refers to expertise in digital literacy, ethics, etiquette, online safety, norms, rights, culture, and other related areas. A digital citizen is someone who understands what constitutes appropriate and inappropriate behavior online, demonstrates smart technology behavior, and makes sound decisions when using technology.

Starting from the basic concept of citizenship, that permanent political and legal bond between a person and a particular state, we propose to examine the concept in terms of its digital component.

Thus, this bond is expressed by all mutual rights and obligations between a person and the state of which he or she is a citizen. While citizenship can be acquired mainly by birth or naturalization, digital citizenship is a right that is acquired with access to the Internet and digital equipment. We can therefore interpret digital citizenship not as a legal concept, but as a technical

---

[287] The European Commission for the Efficiency of Justice, a branch of the Council of Europe, approved the first set of ethical guidelines in 2018 for the use of artificial intelligence in judicial systems. The guidelines are known as the" European Ethical Charter on the use of artificial intelligence in and related to the judiciary".

[288]Veronica Dobozi, *Carta etică europeană cu privire la utilizarea inteligenței artificiale în sistemul judiciar și în legătură cu acesta,* https://www.juridice.ro, (25.01.2023)

[289]European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe, *European Ethical Charter on the Use of Artificial Intelligence in Legal Systems and their Environment*, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, (25.01.2023)

[290]Council of Europe, *Internet Education (Literacy) Manual,* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/internet-handbook-ro/16809f0b11, (25.01.2023)

one, and we can even include it in the category of citizenship for a fee[291], whereby citizenship can be obtained for a certain amount of money, but this time the cost is not imposed by programs that offer foreign investors the opportunity to obtain citizenship, but by the obligation of each state to ensure that the design and implementation of the corresponding artificial intelligence technologies and the services offered are compatible with the fundamental rights of citizens, but also by regulations on digital services, such as the Digital Services Regulation[292] which includes rules for online intermediary services, which millions of Europeans use every day.

In the European context, the European Union, a supranational entity, has started to develop more and more chapters on "new technologies". Due to digital dependencies[293] (telecommunications, mobile telephony, Internet, computers, microprocessors, data, etc.), the European digital public space is limited by the concept of **digital sovereignty**.

Sovereignty[294] is that inherent, inalienable, and indivisible attribute of the state, which consists of the supremacy of state power within its borders and its independence in relations with other states. It should be noted that the territorial limit of state sovereignty limits public space but not digital space. However, digital space is itself an essential economic resource for the fourth industrial revolution, so territorial and material barriers, and limits are subject to national, European, and international regulations.

Daniel Lambach and Kai Oppermann conducted an empirical analysis of the phenomenon of digital sovereignty[295]. In the published study both positive (benefits and opportunities) and negative (risks and challenges) references for digitization were presented. Reference was also made to the threats to digital sovereignty that may arise from digitization. In terms of narrative characters[296], the authors have described three types of actors:

- potential bearers of digital sovereignty;
- agents charged with establishing or protecting digital sovereignty;
- agents charged with establishing or protecting digital sovereignty.

The holders and agents of digital sovereignty have been divided into societal, individual, or collective actors (such as individual citizens or consumers as well as society at large), economic actors (including companies and industries), and EU public actors (such as institutions and government agencies).

Focusing on the negative references of digitization, but also on the threats to digital sovereignty, we would also like to draw attention to "computerized battles for influence", a new component of **cyber defense**, aimed at countering information manipulation and countering propaganda maneuvers. The conflict in Ukraine is a perfect illustration of the impact of this form of action, which is primarily the responsibility of the state[297]. In these circumstances, cooperation between the public and private sectors is essential, as many solutions are in the hands of companies and security providers.

---

[291]Shora Azarnoush, Claudia Stefan, *Preţuri mari pe piaţa naţionalităţilor*, adevarul.ro/blogurile-adevarul/preturi-mari-pe-piata-nationalitatilor-1554527.html, (25.01.2023)

[292]European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending the Directive 2000/31/CE*, COM/2020/825 final, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52020PC0825, (25.01.2023)

[293]European digital industries are seen as lagging their American and Chinese competitors. US-built platforms have created oligopolies that threaten the security of European users' data.

[294]Reference definition: sovereignty. https://dexonline.ro/definitie/suveranitate, (25.01.2023)

[295]Daniel Lambach, Kay Oppermann, *Naraţiuni ale suveranităţii digitale în discursul politic german*, 2022, https://onlinelibrary.wiley.com/doi/10.1111/gove.12690, (25.01.2023)

[296]*Idem*

[297]Marc Watin-Augouard, *Securitatea cibernetică - o condiţie sine qua non pentru "deceniul digital" al UE*, 2022, https://www.bursa.ro/securitatea-cibernetica-o-conditie-sine-qua-non-pentru-deceniul-digital-ale-ue-41975642, (26.01.2023)

Given the above, the digital space extends the obligations of the classical concept of sovereignty as argued by the authors of the Tallinn Manual 2.0 " Cyber activities take place on territory and involve objects, or are conducted by persons or entities, over which States may exercise their sovereign prerogatives"[298].

Despite the perception of a borderless cyberspace, individuals' activities are still subject to the jurisdiction of the state. Presently, many nations apply their national laws to actions conducted in the digital realm, particularly in cases where cybercrime has a tangible real-world counterpart, such as intellectual property or identity theft, financial fraud, human trafficking, or unauthorized access to sensitive data.[299]

The European Union, and the European Commission, have adopted the interpretation of digital sovereignty as the control of the "resource regime" about data by developing a regulatory environment that structures the interactions between market actors[300]. The proposed Data Governance Act[301] (DGA) includes elements of data access control and localization.

Digital sovereignty gets a real sense of state, even supranational, control if we look at the new set of rules of the sharing economy[302] and the emergence of new entities, technology companies that mediate more and more of our social and economic interactions and without which we would find it increasingly difficult to function as a society[303].

Internationally, digital supremacy is focused on economic and security stakes and the competition will be won by those companies that will build digital infrastructures on the territory of countries that promote digital democracy. In other words, the aim is to promote user autonomy, because citizens do not have the freedom to choose their data but are simply passive users who receive information based on their profile. From this, we conclude that the "shared economy (in the narrow sense) is not about sharing" but about profit orientation, expected reciprocity, and the absence of feelings of community[304].

As the governments of European states, with a common heritage of political ideals and traditions, respect for freedom, and the rule of law, it is for the European states to take the first steps towards collectively guaranteeing certain rights set out in the Universal Declaration. Digital citizens are users of the world's most important information-sharing service, even if they do not feel any of the mutual obligations that arise when they share their identity, i.e., the fundamental characteristics that distinguish them from all others and make them remain themselves for the whole of their existence, in time and space. In this context, on the 26th of January 2022, the European Commission proposed a solemn inter-institutional declaration on

[298]Michael N. Schmitt (ed.), *Manualul Tallinn 2.0 privind dreptul internațional aplicabil operațiunilor cibernetice*, Cambridge University Press, 3rd of February 2017, https://doi.org/10.1017/9781316822524, (04.04.2023)

[299]Cosmina Moghior, *Suveranitatea digitală europeană: o analiză a delegației de autorități*, in "Romanian Journal Of European Affairs", Vol. 22, No. 1, 2022, p.108

[300]Pascal König, *Analizarea guvernanței datelor în UE prin prisma conceptului de regim al resurselor*, 2022, https://www.ssrn.com/abstract=4050804, (25.01.2023)

[301]European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, COM/2020/767 final, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767, (25.01.2023)

[302]Sebastian Vith, Achim Oberg, Marcus A. Höllerer, Renate E. Meyer, *Vizionarea „Orașului partajat": stategii de guvernare pentru economia partajată,* in "Jurnalul de etică în afaceri", Vol. 159, 2019, pp. 1023–1046, https://link.springer.com/article/10.1007/s10551-019-04242-4, (26.01.2023)

[303]Mirela Mărcut, *Spațiul digital nu e ca spațiul cosmic. Despre suveranitatea digitală*, in "Digital", European Union, https://digitalpolicy.ro/2021/05/22/spatiul-digital-nu-e-ca-spatiul-cosmic-despre-suveranitatea-digitala, (26.01.2023)

[304]Giana M. Eckhardt, Fleura Bardhi, *The sharing economy isn't about sharing at all*, in "Harvard Business Review", 2015, https://hbr.org/2015/01/the-sharing-economy-isnt-about-sharing-at-all, (26.01.2023)

digital rights and principles for the digital decade[305]. The digital rights and principles described in the declaration will supplement current rights, including those stemming from the EU Charter of Fundamental Rights and data protection and privacy regulations. The suggested rights and principles focus on a people-centric digital transformation, encompassing freedom of choice, safety and security, solidarity and inclusion, participation, and sustainability.

Moreover, "the Commission will soon propose a secure European electronic identity. An identity that we can trust, and that any citizen can use anywhere in Europe for everything from paying taxes to renting a bike. A technology where we can control for ourselves what data is used and how it is used"[306].

The European Digital Identity is scheduled to be accessible to citizens, residents, and businesses of the European Union who wish to authenticate their identity or corroborate certain personal details. It will be able to be used to purchase both public and private services, either online or offline, throughout the EU[307]. Digital identity will give anyone a simple and secure way to control shared information and will work through digital wallets available as apps on smartphones and other devices[308].

Digital identity is seen as an extension of national or European identity, while digital citizenship is an extension of the conventional concept of citizenship. Digital sovereignty refers to a nation's ability to control and protect its own digital activities, information, and resources. Essentially, it is about a state's ability to protect its sovereignty in the digital space, as well as promote and defend its interests in terms of digital policy.

In the European context, sovereignty is based on the principle that each member state must digitally protect and manage its digital resources. However, transaction costs and the credibility of political commitments may mean that some aspects of digital policies are managed at the supranational level. For example, the European Union (EU) promotes common policies and regulations regarding cyber security, data protection, and digital rights, to ensure that all member states follow the same standards and practices. In addition, supranational institutions such as the European Commission may be tasked with managing specific aspects of digital policy, such as the coordination of EU-wide digital infrastructure. In general, digital sovereignty in Europe involves finding a balance between protecting national sovereignty and coordinating and collaborating on digital policy at the supranational level.

The concept of digital sovereignty involves a nation's ability to protect and control its digital activities and resources, but it can also have a wider impact on the geopolitical scene. Currently, there is a global competition for dominance over the "digital model", which involves different perspectives and objectives regarding the role of technology in the interaction between the state, citizens, and the economy. Some countries want to have a dominant role. The normative interpretation of the triangular relationship between the European Union, the United States, and China is a critical component of digital geopolitical competition. The EU champions

---

[305]Comisia Europeană, *Deceniul digital al Europei: obiective digitale pentru 2030*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_ro, (26.01.2023)

[306]Ursula von derLeyen, President of the European Commission, in her State of the Union address, 16 September 2020

[307]EU Council, Press release 6 December 2022, *European Digital Identity (eID): Council makes progress towards EU digital wallet, a paradigm shift for digital identity in Europe*, https://www.consilium.europa.eu/ro/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/, (26.01.2023)

[308]European Commission, *European Digital Identity*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_ro, (26.01.2023)

a technological model based on "democratic values, respect for the rule of law and fundamental rights"[309].

In contrast, the United States maintains a relatively hands-off approach to technological progress, preferring to let the private sector self-regulate and standardize with minimal government intervention. In contrast, China represents the other end of the spectrum, strongly supporting the extension of traditional principles of digital sovereignty but the government exercising exclusive authority over all non-state entities and other governments operating in their national cyberspace[310].

Digital sovereignty is a source of power, also at the European level.

In essence, sovereignty involves giving power to the state to govern and control the territory and resources within a given area. In the context of European digital affairs, it is not immediately clear who holds this power. The typical model for power delegation is the principal-agent theory, where the state is the principal and citizens are the agents[311]. This theory is based on an economic theory, according to which the principal will look for an agent to carry out certain activities for which the principal does not have the necessary resources (in particular, the emphasis is on the principal's lack of expertise and the fact that the agent has much more information on specific areas of activity)[312].

The concept of delegation refers to a hierarchical and dyadic relationship between two parties, the principal and the agent. The principal delegates his responsibility or authority to the agent to act on his behalf or to perform certain tasks. This relationship is interdependent because the success of the agent depends on the success of the main goals. The agent has his preferences and interests which may or may not align with those of the principal. If the agent's preferences align with those of the principal, agents will be more willing to follow the principal's instructions without the need for incentives or sanctions. However, when the agent's interests do not align with those of the principal, it may be necessary to use appropriate rewards or sanctions to keep the agent on track.

The agent's preferences and interests are influenced by his personal value system, which may differ from that of the principal. These differences in the agent's identity characteristics can influence how he exercises his authority and how he performs his tasks. Therefore, the principal must have a clear understanding of the agent's values and motives to communicate with the agent in a way that encourages the desired behavior.[313]

The theory mentioned above clarifies why EU Member States are inclined to transfer more authority to supranational organizations. The primary motives for this are to minimize transaction costs related to information, negotiation, and implementation, as well as to enhance the credibility of policy commitments by making a long-term commitment to critical

[309]European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint *Communication to the European Parliament, the European Council and the Council: EU Cyber Security Strategy for the Digital Decade*, Brussels, 2020, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52020JC0018&from=EN, (26.01.2023)

[310]Rogier Creemers, *Concepția Chinei despre suveranitatea cibernetică: retorică și realizare,* in D. Broeders& Berg B. van den (Eds.) "Guvernarea spațiului cibernetic: comportament, putere și diplomație. Tehnologii digitale și politică globală", Lanham, Rowman&Littlefield, 2020, pp. 107-142

[311]Cosmina Moghior, *Suveranitatea digitală europeană: o analiză a delegației de autorități*, in "Romanian Journal of European Affairs", Vol. 22, No. 1, 2022, p.109

[312]David G. Hawkins et al. (eds.), *Delegation and Agency in International Organizations*, Cambridge University Press, 2006, online 2009, https://doi.org/10.1017/CBO9780511491368, (04.04.2023)

[313]Simona Claudia Crețа, *Problema delegării şi relaţiile dintre politicieni şi birocraţi*, in "Revista Transilvană de Ştiinţe Administrative", 1(10), 2004, pp. 19-24

legislation[314]. In the same sense, digital sovereignty provides additional incentives for delegating powers. The concept, therefore, facilitates compromise in the virtual world.

The European Communities created the common market, which has become a single market, now the European Union must access the program plan "for the digital decade" presented in March 2021. But the red thread of respect for national and supranational sovereignty is cyber security, which is not an end but a condition based on common values.

Conclusions

Regardless of the state of progress of new technologies, we must work together as digital citizens, to be present at this great event, the digitization of society, to share our knowledge, to build an efficient legal system, and to propose well-thought-out and analyzed solutions. Social needs are essential for both the private and public existence of individuals and communities. The future depends on understanding the concept of the digital citizen in conjunction with the concept of digital sovereignty, i.e., how the digital citizen proposes to respect the limits of the application of the digitization of public space in all sectors of activity.

Digital security thus becomes a prerequisite for the existence and proper functioning of democratic societies at the regulatory, executive, and jurisdictional levels.

We conclude that digital sovereignty, digital citizenship, and digital identity, from a normative point of view, are terms that translate into ideas, political, and even metaphorical understandings.

Bibliography

Books

1. Dragoman, Dragoș, *Declinul democratic din România după 2007*, TehnoMedia, Sibiu, 2022
2. Habermas, Jurgen, *Sfera publică și transformarea ei structurală*, Comunicare.ro, București, 2005

Articles

1. Creemers, Rogier*, Concepția Chinei despre suveranitatea cibernetică: retorică și realizare*, in D. Broeders&Berg B. van den (Eds.), "Guvernarea spațiului cibernetic: comportament, putere și diplomație. Tehnologii digitale și politică globală", Lanham, Rowman&Littlefield, 2020
2. Creța, Simona, Claudia, *Problema delegării şirelaţiile dintre politicieni şi birocraţi*, in "Revista Transilvană de Ştiinţe Administrative", 1(10), 2004
3. Eckhardt, Giana,M.; Bardhi, Fleura, *The sharing economy isn't about sharing at all*, in "Harvard Business Review", 2015
4. Hawkins, David; et al., (eds), *Delegation and Agency in International Organizations*, Cambridge University Press, 2006
5. Johnson, Pauline, *Habermass Search for the Public Sphere*, in "European Journal of Social Theory", Vol. 4, No. 2, 2001
6. König, Pascal, *Analizarea guvernanței datelor în UE prin prisma conceptului de regim al resurselor*, 2022
7. Lambach, Daniel; Oppermann, Kai, *Narațiuni ale suveranității digitale în discursul politic german*, 2022
8. Mărcuț, Mirela, *Spațiul digital nu e ca spațiul cosmic. Despre suveranitatea digitală*, in "Digital", European Union
9. Moghior, Cosmina, *Suveranitatea digitală europeană: o analiză a delegației de autorități*, in "Romanian Journal of European Affairs", Vol. 22, No. 1, 2022

[314]Cosmina Moghior, *Suveranitatea digitală europeană: o analiză a delegației de autorități*, in "Romanian Journal of European Affairs", Vol. 22, No. 1, 2022, p.109

10. Munteanu, Nicoleta, Annemarie, *Illegal migration approach from the perspective of open source intelligence (OSINT)*, in "Research and Science Today", No. 2 (18)/2019
11. Schmitt, Michael, N., (ed.), *Manualul Tallinn 2.0 privind dreptul internațional aplicabil operațiunilor cibernetice,* Cambridge University Press, 3rd of February 2017
12. Vith, Sebastian; Oberg, Achim; Höllerer, Marcus, A.; Meyer, Renate, E. *„Orașului partajat": stategii de guvernare pentru economia partajată*, in "Jurnalul de etică în afaceri", Vol. 159, 2019
13. Watin, Augouard, Marc, *Securitatea cibernetică - o condiţie sine qua non pentru "deceniul digital"* al UE, 2022

Legislation and Documents

1. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions. A Digital Single Market Strategy for Europe*, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52015DC0192
2. European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council and the Council: EU Cyber Security Strategy for the Digital Decade, Brussels, 2020,* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52020JC0018&from=EN
3. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending the Directive 2000/31/CE, COM/2020/825*, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52020PC0825
4. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final, 2020*
5. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, COM/2020/767 final, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767
6. *Regulation (EU) 2018/302 of the European Parliament and the Council of 28 February 2018 on the prevention of unjustified geo-blocking and other forms of discrimination based on nationality or nationality, domicile, or the registered office of customers in the internal market and amending Regulations (EC) No. 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC*, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32018R0302

Reports and Studies

1. ADR, *Transformarea digitală a instituțiilor publice*, https://www.adr.gov.ro/transformarea-digitala-a-institutiilor-publice/
2. Comisia Europeană, *Deceniul digital al Europei: obiective digitale pentru 2030*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_ro
3. Council of Europe, *Internet Education (Literacy) Manual,* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/internet-handbook-ro/16809f0b11
4. Daniel Lambach, Kay Oppermann, *Narațiuni ale suveranității digitale în discursul politic german*, 2022, https://onlinelibrary.wiley.com/doi/10.1111/gove.12690
5. EU Council, Press release 6 December 2022, *European Digital Identity (eID): Council makes progress towards EU digital wallet, a paradigm shift for digital identity in Europe*, https://www.consilium.europa.eu/ro/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/
6. *EU's response to the "Arab Spring": The State-of-Play after Two Years, official EU document*, 8 February 2013, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/135292.pdf.
7. European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe, *European Ethical Charter on the Use of Artificial Intelligence in Legal Systems and their Environment*,

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c
8. European Commission, *European Digital Identity*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_ro
9. Marc Watin-Augouard, *Securitatea cibernetică - o condiţie sine qua non pentru "deceniul digital" al UE*, 2022, https://www.bursa.ro/securitatea-cibernetica-o-conditie-sine-qua-non-pentru-deceniul-digital-ale-ue-41975642

Websites

1. https://commission.europa.eu/
2. https://digitalpolicy.ro/
3. https://eur-lex.europa.eu/
4. https://eur-lex.europa.eu/
5. https://link.springer.com/
6. https://onlinelibrary.wiley.com
7. https://www.adr.gov.ro/
8. https://www.bursa.ro/
9. https://www.chinadaily.com
10. https://www.consilium.europa.eu/ro/