https://doi.org/10.18485/iipe_euchanges.2021.ch5

EUROPEAN UNION'S QUEST FOR DIGITAL SOVEREIGNTY: POLICY CONTINUATIONS AND STRATEGY INNOVATIONS

Mihajlo VUČIĆ[1]

Abstract: The paper deals with the EU "digital sovereignty" defined as a capacity to influence norms and standards of the information technology in order to preserve the integrity of the internal market, foundational EU values, and the capacity to act as an independent entity in the geopolitical struggle among the great powers for control of the digital sphere. Digital sovereignty was set as a top priority for the next mandate of the European Commission. The article treats the efforts of the EU to achieve digital sovereignty in three interrelated fields such as digital economy, data protection and artificial intelligence, based on the author's assumption that traditional normative and economic clout of the EU gives it the best chances to succeed quickly exactly in these fields. The author analyses the various legislative acts either adopted or proposed by EU authorities in the field of digital markets and services and their intended effects on major multinationals in the digital economy as a continuation of previous EU efforts in the competition and data protection fields, where the main idea is to protect the integrity of the single market and human rights of EU citizens. In the field of artificial intelligence, in addition to these aims, there is also the wish to engage in strategic competition with China and the US and to offer a third path, one based on the EU values that might attract a following among other states.

Keywords: EU, digital sovereignty, digital markets, data protection, digital services, artificial intelligence.

---

[1] Research Fellow, Institute of International Politics and Economics, E-mail: mihajlo@diplomacy.bg.ac.rs.

The paper presents findings of a study developed as a part of the research project "Serbia and challenges in international relations in 2021", financed by the Ministry of Education, Science, and Technological Development of the Republic of Serbia, and conducted by the Institute of International Politics and Economics, Belgrade.

INTRODUCTION

Regulation of the digital sphere is not a new topic for the European Union (EU), but regulation with the purpose of achieving sovereignty in this sphere, on the contrary, is a rather recent phenomenon. Take, for example, electronic commerce, which has been regulated by a Directive on e-commerce 2000,[2] at a time when major digital companies were in the early infancy (Google was just two years old) or at best in the minds of its creators (Facebook appeared in 2004). Nowadays, its rules have become obsolete for the most purposes of contemporary digital regulation, and what is even more important for the purpose of this article, they were certainly never intended to provide any notion of strategy or sovereignty in the digital sphere, but rather were used as a tool to regulate the business on the internal market in the usual, *laissez-faire* approach of economic liberalism and fair-play (Blankertz and Jaursch, 2020).

This approach, in general, has not proved convenient for the EU's ability to control its own development in the digital sphere, since the EU is primarily an economic powerhouse, with the internal market as the greatest asset in the projection of its power in international relations. Thus, the EU must assure this market stays under the control of its institutions, that is, under its sovereignty. However, the realities of the digital age approaching are straying aside from the aspirations that the founding fathers of the digital revolution had in mind. It seems the digital space is no longer just a vehicle for international cooperation, multilateralism, and general democratization of the global society. It rather represents a fertile ground for terrorism (Von Behr et al, 2013), hybrid warfare (Danyk et al, 2017), cybercrime (Carrapico and Farrand, 2020), heavy infringements of human rights, and authoritarian aspirations of various global leaders (Druzin and Gordon, 2017). In other words, there is no place anymore for normative acts that treat the digital economy in this business-as-usual manner the EU is so used to.

Furthermore, the economy and politics in the digital sphere go hand in hand, and other great powers are somehow prone to grasp and accommodate this fact into their politics more readily than the EU. The EU is currently experiencing itself divided and more as a passive observer of the process of

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178, 17.7.2000, p. 1–16.

geopolitical (ab)use of the digital sphere than as the united and active actor in the competitive digital race. On the other hand, other great powers efficiently use the digital sphere for the projection of their influence upon international relations. The "Chinese model" – a market economy under the strong grip of the authoritarian state – has proven itself especially conducive to the efficient use of huge digital corporations, such as Huawei, as geopolitical tools of leverage. (Tekir, 2020). China is the proud owner of the world's most advanced quantum computer and is closing the gap with the United States in the economic and military application of AI (artificial intelligence) (Rahman, 2020). The EU finds itself in between the crushing competition of the two new digital superpowers (US and China). This has repercussions for the economic well-being and respect for human rights of its citizens since they are dependent upon the products, services and technologies of these superpowers, from chat platforms to data storage facilities and telecommunications equipment. This dependence can undermine the economic well-being and human rights if the geopolitical competition between the US and China continues at the same pace, and currently, it definitely seems that this is the case. This would in turn undermine the foundational values of the EU itself and the purpose for which it was created. It would also render impossible in the longer term any meaningful policy implementation in the framework of the Common Foreign and Security Policy since the EU institutions would be left without independent means to implement this policy in the digital age and instead relying on the goodwill and interests of one of the superpowers to whom they would attach. "The questions of who owns the technologies of the future, who produces them, and who sets the standards and regulates their use have become central to geopolitical competition" (Shapiro, 2020, pp. 6-7).

In this context, the idea of digital sovereignty is part of a wider debate and activity to maintain the EU's capacity to act independently on the world stage to protect the interests of its citizens in the atmosphere of increasing geopolitical competition on a host of issues, from armaments race, trade and investment, resources and markets grab, to health and security, etc. This accelerating competition is coupled with the popular US pivot to the Pacific and a consequential lack of interest for the protection of EU interests (Davidson, 2014). In some instances, it is exacerbated by the ever more obvious focus of the US upon its own economic interests, which leads it to regard the EU not as an ally but as a competitor due to its economic power (Hackenbroich, 2020). The EU is looking for its own path, and it tries to leverage the humanistic values upon which it was founded to create a general framework to guide the policy formulation and implementation in

this field. This general framework can then be applied to various manifestations of digital policy: internet governance, 5G infrastructure security, data management and protection, artificial intelligence usage, disinformation prevention and mitigation, and finally the issue of broadband capacity. Of all these manifestations, this article chooses to concentrate on three interrelated issues – data sovereignty, artificial intelligence "with a European touch", and internet governance in the digital market sphere since it is the opinion of the author that those three fields are the most promising for the EU's quest to achieve the digital sovereignty. This opinion is grounded in the assumption that the EU's abilities to achieve digital sovereignty are primarily its regulatory and institutional powers and a rich and profitable internal market. The ability to shape the international environment on digital issues through quality normative models and effective institutional application and enforcement of these models, in combination with the internal market power of attraction enables the capacity to influence the norm-setting practices of other states.

DIGITAL SOVEREIGNTY AS AN UPGRADE OF ANALOGUE SOVEREIGNTY

The distinction between national or supranational sovereignty is an important issue for the EU since it reflects the usual dynamic of power relationships in this complex institutional entity. Does digital sovereignty relate to the national sovereignty of a particular member state or is it really about the EU as a whole, and if is, is that the realistic proposal? How are the competencies between the EU and its member states divided when it comes to the policies required to achieve digital sovereignty? The answer is not a straight one. The traditional or, let us say, "analogue" sovereignty in the EU is split between the supranational and the member state levels, with some parts of it staying in between. Therefore, sovereignty can be split into three categories, exclusive competences of the EU, shared competences, and the exclusive competences of a member state. For example, "tax policies remain in the national remit, which implies that the multinational digital companies can exploit this to its advantage and play out national sovereignties against each other" (Floridi, 2020, p. 375). On the other hand, monetary sovereignty has largely become supranational, at least for those member states that have adopted the euro. It is probably to be expected that this mixture of sovereignties will be applied to the digital realm as well. This will largely depend on the functional criteria, meaning that in those fields of policies where the EU is better placed to act, digital sovereignty will manifest as

supranational, while in some others, the member states themselves would keep the independence to act.

Thus, for example, digital data sovereignty has already become an EU sovereign policy, through the adoption and vigorous implementation of the General Data Protection Regulation (GDPR). Only in 2020, the GDPR provisions were enforced more than 150 times by the EU or the member states authorities against multinational companies, of which a substantial number was actually established outside the EU. One of the biggest fines were enforced against *Google* (over 50 million euros) (Majstorović, 2020, p. 114). The GDPR basically prevents foreign companies from pulling the sovereignty over digital data out of the hands of the EU citizens. "Due to its strong extra-territorial effect, it is applicable to and enforceable over any company wishing to pursue business inside the internal market or otherwise having substantial effects upon the EU citizens or residents" (Vučić, 2020, pp. 44-47). The attraction of the internal market and the strong normative power of the EU institutional framework combine to provide digital sovereignty over data in this case.

This is something already seen in other policy fields, such as competition, where the EU Commission has a rich and long-standing practice of extra-territorially applying and enforcing competition provisions of the EU legislation over companies from all over the world defending this application and provision through the so-called *effects doctrine*, which basically provides that any anti-competitive behaviour in the global economy which causes the substantial effect to the functioning of the internal market falls under the jurisdiction of the EU law (Gerardin et al, 2011, pp. 21-26).[3] Both the competition and data protection policies have the additional purpose of strategically positioning the EU as the normative and value-based role-model for other states, ensuring that the EU remains sovereign in its pursuit of specific rules and values for the protection of human rights, free market principles, and democracy. Their power of enforcement has

[3] For landmark cases of the application in practice of the effects doctrine see: *Imperial Chemical Industries Ltd. v. Commission of the European Communities* (*Dyestuffs*), ECJ judgment, Case 48/69, Imperial Chemical Industries Limited v. Commission [1972] E.C.R. 619; *In re Wood Pulp Cartel,* 1985 O.J. (L 85) 1, [1985] 3 C.M.L.R 474 (1985); *Gencor*, Judgment of the General Court, Case T-102/96, Gencor v. Commission, [1999] E.C.R. II-753; *Grosfillex-Fillistorf* [1964] 3 CMLR 237; and the most important in recent years *Intel*, Case C-413/14 P, Intel Corporation v European Commission, ECLI: EU: C: 2017:632.

been proven time and again in practice. Just to illustrate with one prominent example, in the period 2017-2020 the Commission fined three times a US-based digital-giant *Google* for its anti-competitive behaviour influencing the internal market and consumer rights of EU citizens and businesses, and the damages awarded totaled around 8.2 billion euros.[4]

DIGITAL MARKETS AND SERVICES

The policy fields of data protection and competition have been moved during the last year in the direction of an additional digital upgrade. The European Commission unveiled two long-awaited legislative proposals— the Digital Services Act (DSA)[5] and the Digital Markets Act (DMA).[6] These two acts combined represent the cornerstone of the European digital strategy, a policy document of the EU Commission unveiled in February 2020, which states as its main aim the establishment of the EU as a global role model for the digital economy, through the development of digital standards in line with European values.[7] The Digital Strategy builds upon the results achieved in the period 2014-2019 when the Commission pushed through various legislative proposals for boosting e-commerce, e-Privacy, IP protection, the harmonization of digital rights, harmonized VAT rules, and cyber security as part of its "Digital Single Market" strategy.[8]

[4] See cases: Case AT.39740 — Google Search (Shopping), C(2017) 4444, OJ C 9, 12.1.2018, pp. 11–14; Case AT. 40099 — Google Android, C(2018) 4761, OJ C 402, 28.11.2019, pp. 19–22; and see for third case the press release relating details of the case available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770, 20.1.2021.

[5] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN, 20.1.2021.

[6] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final, retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN, 20.1.2021.

[7] European Commission, "Shaping Europe's Digital Future", February 2020, retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/fs_20_278, 20.1.2021.

[8] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions:

While the EU Treaties do not contain any special provisions on information and communication technologies, the EU is allowed to take relevant actions within the framework of sectoral and horizontal policies.[9] All these are among the key elements for a digital Europe. Therefore, the legal basis for the DMA and DSA was found in Article 114 TFEU,[10] which ensures the functioning of the internal market. In our opinion, the EU has the most potential to prosper in its quest for digital sovereignty through the implementation of these two pieces of legislation since they build upon a successful past practice of application and enforcement of competition and privacy laws, guaranteed by the powers of attraction of the economic clout of the internal market and normative role-model of the EU's data protection policies. Therefore, we will concentrate a little bit longer on their provisions and how are they expected to function in practice.

Digital services are in the essence of cross-border nature. The new rules will limit regulatory fragmentation of digital services, in particular in relation to gatekeeper platforms, and reduce compliance costs for companies operating in the internal market. The DMA establishes a set of narrowly defined objective criteria for qualifying a large online platform as a so-called "gatekeeper". These criteria will be met if a company: 1) has a strong economic position, significant impact on the internal market, and is active in multiple EU countries;[11] 2) has a strong intermediation position, meaning that it links a large user base to a large number of businesses;[12] 3) has (or is about to have)

A Digital Single Market Strategy for Europe, COM/2015/0192 final, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192, 20.1.2021.

[9] Such as industrial policy; competition policy; trade policy; the trans-European networks; research and technological development and space; the approximation of laws for improving the establishment and the functioning of the internal market; the free movement of goods; the free movement of people, services and capital; education, vocational training, youth and sport.

[10] "Treaty on the Functioning of the European Union", consolidated version, OJ C 326, 26.10.2012, pp. 47–390.

[11] This is presumed to be the case if the company achieves an annual turnover in the European Economic Area (EEA) equal to or above € 6.5 billion in the last three financial years, or where its average market capitalization or equivalent fair market value amounted to at least € 65 billion in the last financial year, and it provides a core platform service in at least three Member States.

[12] This is presumed to be the case if the company operates a core platform service with more than 45 million monthly active end users established or located in the

an entrenched and durable position in the market, meaning that it is stable over time.[13] The potential addressee of the DMA is a large multinational corporation whose activities, in the long run, cause direct and substantial effects on the functioning of the internal market and the livelihoods of multiple EU citizens. These companies control at least one so-called "core platform service" (such as search engines, social networking services, certain messaging services, operating systems and online intermediation services), and have a lasting, large user base in multiple countries in the EU.

Once identified as the gatekeeper, the company will carry an extra responsibility to conduct itself in a way that ensures an open online environment that is fair for businesses and consumers, and open to innovation by all, complying with specific obligations laid down in the draft legislation. Some examples include: allowing third parties to inter-operate with the gatekeeper's own services; providing the companies advertising on their platform with access to the performance measuring tools of the gatekeeper and the information necessary for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper; allowing their business users to promote their offers and conclude contracts with their customers outside the gatekeeper's platform; providing their business users with access to the data generated by their activities on the gatekeeper's platform. Gatekeepers may no longer block users from un-installing any pre-installed software or apps; may not use data obtained from their business users to compete with these business users, and may not restrict their users from accessing services that they may have acquired outside of the gatekeeper platform.

The DMA is not a toothless piece of legislation since, in order to ensure the effectiveness of the new rules, the possibility of sanctions for non-compliance with the prohibitions and obligations is foreseen. If a gatekeeper does not comply with the rules, the Commission can impose fines of up to 10% of the company's total worldwide annual turnover and periodic penalty payments of up to 5% of the company's total worldwide annual turnover. In case of systematic infringements, the Commission can impose additional remedies. Where necessary to achieve compliance, and where no alternative, equally effective measures are available. These can include structural

EU and more than 10 000 yearly active business users established in the EU in the last financial year.

[13] This is presumed to be the case if the company met the other two criteria in each of the last three financial years.

remedies, such as obliging a gatekeeper to sell a business or parts of it (i.e., selling units, assets, intellectual property rights, or brands).

Given the cross-border nature of gatekeepers and the complementarity of the DMA with the DSA and other internal market rules and competition law, in particular, the enforcement of the tool will remain in the hands of the Commission. The Member States may always request the Commission to open a market investigation for the purpose of designating a new gatekeeper. Besides, DMA is a Regulation, containing precise obligations and prohibitions for the gatekeepers in scope, which can be enforced directly in national courts. This will facilitate direct actions for damages by those harmed by the conduct of non-complying gatekeepers. The DMA complements the enforcement of competition law at the EU and national levels. The new rules are without prejudice to the implementation of EU competition rules (Articles 101 and 102 TFEU) and national competition rules regarding unilateral behaviour. Regulation and competition enforcement already coexist in other sectors, such as energy, telecoms, or financial services. The DMA addresses unfair practices by gatekeepers that either: 1) fall outside the existing EU competition control rules; 2) cannot always be effectively tackled by these rules because of the systemic nature of some behaviours, as well as the *ex-post* and case-by-case nature of competition law. The DMA will thus minimize the harmful structural effects of these unfair practices *ex-ante*, without limiting the EU's ability to intervene *ex-post* via the enforcement of existing EU competition rules.

The Digital Services Act (DSA) is a complementary act to the DMA which intends to foster innovation, growth and competitiveness, and facilitate the scaling up of smaller platforms, small and medium enterprises and start-ups on the EU digital market. Its provisions are situated into a context of European values, placing citizens at the centre, thus the responsibilities of users, platforms, and public authorities are rebalanced according to these values. The ultimate purpose is to ensure better consumer protection and respect for the fundamental rights online, at the same time establishing powerful transparency and a clear accountability framework for online platforms. This will provide an important aspect of digital sovereignty, since democratic forms of control would ensure the systemic platforms respect the EU legal order, while at the same time manipulation or disinformation, as systemic risks to this democratic sovereignty, would be prevented or at least mitigated.

The addressees of the DSA are companies offering so-called digital intermediary services, in essence, basic network infrastructure: internet

access providers, domain name registrars, hosting services such as cloud and web hosting services, online platforms bringing together sellers and consumers such as online marketplaces, app-stores, collaborative economy platforms and social media platforms. Again, as with the DMA, specific rules are foreseen for platforms reaching more than 10% of 450 million consumers in Europe since they pose particular risks in the dissemination of illegal content and societal harms. The DSA is extra-territorial in nature since it regulates all online intermediaries offering their services in the single market, even if they are established outside the EU.

The mechanisms of the DSA's implementation should serve as an upgrade over the previously existing EU legislation in this field. They will include measures to counter illegal goods, services or content online, such as a mechanism for users to flag such content and for platforms to cooperate with "trusted flaggers". This procedure is inclusive and enables a form of a participative right for users in the digital environment's regulation. Users whose content has been flagged would have the possibility to challenge platforms' content moderation decisions, thus ensuring the principle of *audiatur et altera pars*. Users would be safeguarded in their consumer rights through the establishment of transparency measures for online platforms on a variety of issues, including the algorithms used for recommendations. Complementary to this provision is the one related to the researchers who are allowed access to key data of the largest platforms, in order to understand how online risks evolve. The oversight structure is provided in order to address the complexity of the online space. The EU member states will have the primary role, supported by a new European Board for Digital Services.

Very large platforms would be under additional obligations. They have to act proactively and prevent the misuse of their systems by taking risk-based action and by independent audits of their risk management systems. Furthermore, enhanced supervision and enforcement by the Commission complements the work of the Member States and the European Board, when it comes to large platforms oversight.

For both the DMA and the DSA, the issue of very large platforms or digital giants, multinationals that have a strong influence on the EU's digital sovereignty, is the most controversial, not the least because these are also some of the companies with the biggest lobbying budgets in the EU.[14] These

[14] According to https://lobbyfacts.eu/, The Big 5 Silicon Valley firms which would be hardest hit by new provisions (Google, Apple, Facebook, Amazon, Microsoft, often known as „GAFAM") are among the top lobby spenders in Brussels.

budgets have been recently streamlined into a fierce battle for watering down the enforcement provisions of these two acts. According to a corruption watchdog's report: "since the start of the Von der Leyen Commission, 158 meetings were logged as including discussions on the DMA or DSA", and the highest percentage of these meetings involved Google, Microsoft, Facebook, Apple and Amazon.[15] As the legislative battle passes from the Commission on to Council and Parliament, the lobbying intensifies and becomes less transparent. As Transparency International EU found, "by September 2020, only 44% of MEPs had published their lobby meetings, so likely lobbying has been much higher", while the Council does not have the central obligation to disclose lobby meetings (less than half of the permanent representations to the EU do so voluntarily).[16]

AI WITH A "EUROPEAN" TOUCH AND RELATED ISSUES OF DATA LOCALIZATION

Apart from the digital efforts described above, the EU has embarked upon ambitious policy agendas in the field of artificial intelligence (AI), as another important component of digital sovereignty. Last year saw a publication of the key policy document so far by the European Commission –"AI White Paper", which prompted a discussion by policy experts from member states, civil society and businesses that culminated in the Final Report, published just at the end of last year.[17] The "White paper" endorsed the guidelines of a High-Level Expert Group on AI (AI HLEG), commissioned during the year 2019 by the EU authorities which formulated the concept of the "trustworthy Artificial Intelligence", which is centred mainly around the "human-centric" approach to AI that requires compliance with fundamental rights, whether or not these are explicitly

[15] Corporate Europe Observatory, "Big Tech Lobbying: Google, Amazon & friends and their hidden influence", retrieved from: https://corporateeurope.org/en/2020/09/big-tech-lobbying, 20.1.2021.

[16] "MEPs take steps towards lobby transparency and publish 10,000 meetings", retrieved from: https://transparency.eu/european-parliament-10000-meetings/, 20.1.2021.

[17] European Commission, "Public consultation on the AI White Paper: Final report", November 2020, retrieved from: https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence, 20.1.2021.

protected by EU treaties, such as the Treaty on European Union or by the Charter of Fundamental Rights of the European Union (Jobin et al, 2019, pp. 389-399). This approach follows closely the previously discussed areas of data protection and digital market competition. The "White paper" especially stressed the importance of adopting a flexible, agile regulatory framework limited to "high-risk" applications, in sectors such as healthcare, transport, police, and the judiciary, and focused on provisions related to data quality and traceability, transparency, and human oversight (White Paper on AI, p. 2). Some of the potential rules have already provoked concern among non-EU countries: for example, the possibility that AI systems developed and trained outside of Europe will be required to be retrained with European data ahead of their commercialisation (Renda, 2020, p. 59).

The key resource in the development of the AI industry is a huge quantity of data to fuel the process of machine-learning. Therefore, AI sovereignty is so closely related to data sovereignty that they form two sides of the same coin. So far, data needed for research and innovation in the AI field have been mostly stored on cloud servers located outside the EU borders, on platforms such as *Google* and *Alibaba* (US and Chinese incorporated firms respectively), while just around 20% of available data is stored on EU-based servers (Renda, 2020, p. 58). The Commission envisions in the "White paper" that this situation would shift for 180 degrees to around 80% of data being stored locally if every piece of AI strategy gets implemented (White Paper on AI, p. 13). This would enable the Union to pursue sovereign AI policies by controlling the majority of data resources needed for its development and in turn decrease the dominance of its competitors in the AI data global market. In such an environment the EU will have a chance to compete through technologically cutting-edge infrastructure based on a federated cloud, a cloud infrastructure that can accommodate various heterogeneous cloud services under a common set of interoperability specifications (Renda, 2020, p. 58). Some proposals for such a cloud have been already put forward by the German Ministry for Economic Affairs and Energy – the so-called "Gaia-X",[18] and currently it

[18] Federal Ministry for Economic Affairs and Energy (BMWi), "Project GAIA-X—A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem", 2019, retrieved from: https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4, 20.1.2021. Interestingly enough, in the Ministry's document, digital sovereignty is defined

seems that the imagined EU-wide cloud would be based on this technology. Large cloud operators from non-EU countries have already recognised that being admitted to the future European federated cloud infrastructure will imply adhering to a set of protocols and standards that embed compliance with European rules, starting with privacy but also encompassing the forthcoming requirements for high-risk AI applications. (Renda, 2020, p. 60). Similarly, the data spaces announced in the EU strategy for AI will incorporate the EU acquis – the body of common rights and obligations that are binding on all EU countries – as software code (Renda, 2020, p. 61).

In order to create the EU-wide infrastructure needed for this undertaking, the Data Strategy,[19] a Commission communication released on the same day as the White Paper, aims to integrate the national data markets of the member states into a single market for data that will allow it to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations. The first legislative proposal to come from this strategy is a Regulation on European data governance.[20] It aims to boost data sharing across sectors and the Member States, strengthen mechanisms to increase data availability, and overcome technical obstacles to the reuse of data. If adopted, it will support the set-up and development of common European data spaces in strategic domains, involving both private and public players: health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills.

CONCLUSION

The aspects of the quest for digital sovereignty analysed above tell us a two-part story of how the EU is adapting its traditional tools for power

not only as state sovereignty, but also as encompassing the power of companies to freely determine the use and structure of their digital systems, data and processes.

[19] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data, COM/2020/66 final, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066, 20.1.2021.

[20] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767, 20.1.2021.

projection to new digital realities. The first part is related to the traditional *effects doctrine* that was invented to tie the companies operating on the single market to the jurisdiction of the EU institutions in competition law cases. It has been accepted as the leading idea behind a plethora of legislation adopted or proposed by the Commission to implement its strategy for achieving digital sovereignty. Fines for behaviour that distorts the EU rules of play in the digital single market have as its ultimate goal the creation of the level-playing field, or "filling-in the economic gap between the EU companies and American and Asian technology giants" (Celeste and Fabrini, 2020, 56). Due to the attraction of doing business on the internal market, these giants are prone to pay the fines and accept the imposed rules of play. Therefore, the GDPR, the DMA and the DSA with their elaborate systems of enforcement can be expected to continue in locked step with this well-defined practice.

The second part is related to the ever-deepening integration of the common European space based on common values of human rights, free market and democracy to create a uniform bloc that can compete with its much more monolithic adversaries (primarily the US and China) in pursuing the fruits of the new technological revolution. In this part, the main role is given to the concepts of data localization and "trustworthy AI" (or what we have called "AI with a European touch"). Although less developed than the previous part, it builds upon similar examples from analogue reality – forging its own path and waiting for others to follow it as a role-model. The unity of the member states as opposed to the foreign interference will in the end enable this strategy to prosper. If they go through with Commission proposals and allow the free flow of data over the internal borders, while at the same time opting for creating a "Gaia-X" or similar federated cloud infrastructure instead of leaving their data in possession of foreign-based cloud services, sovereignty would be preserved and might serve "as a third path between the laissez-faire US approach and authoritarian Chinese model" (Vučić, 2020, 54), attracting other like-minded states in the process and projecting EU normative power ever further.

REFERENCES

Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising, 20 March 2019, retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770, 20.1.2021.

Blankertz A. and Jaursch J. (2020) How the EU plans to rewrite the rules for the internet. Brookings, retrieved from https://www.brookings.edu/techstream/how-the-eu-plans-to-rewrite-the-rules-for-the-internet/, 20.1.2021.

Carrapico H. and Farrand B. (2020) Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. *Journal of European Integration*, 42(8), pp. 1111-1126.

Case AT.39740 — Google Search (Shopping), C(2017) 4444, OJ C 9, 12.1.2018, pp. 11–14.

Case AT. 40099 — Google Android, C(2018) 4761, OJ C 402, 28.11.2019, pp. 19–22.

Celeste E. and Fabbrini F. (2020) Competing Jurisdictions: Data Privacy across the Borders. In: T. Lynn et al. (eds.) *Data Privacy and Trust in Cloud Computing*, Palgrave MacMillan, 2020.

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, COM/2015/0192 final, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192, 20.1.2021.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data, COM/2020/66 final, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066, 20.1.2021.

Corporate Europe Observatory, "Big Tech Lobbying: Google, Amazon & friends and their hidden influence", retrieved from https://corporateeurope.org/en/2020/09/big-tech-lobbying, 20.1.2021.

Danyk Y. and Maliarchuk T. and Briggs C. (2013) Hybrid War: High-tech, Information and Cyber Conflicts. *Connections*, 16(2), pp. 5-24.

Davidson J. (2014) The U.S. "Pivot to Asia". *American Journal of Chinese Studies*, 21, pp. 77-82.

Druzin B. and Gordon G.S. (2018) Authoritarianism and the Internet. *Law and Social Inquiry*, 43(4), 1427-1457.

European Commission (2002). Public consultation on the AI White Paper: Final report, November 2020, retrieved from: https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence, 20.1.2021.

European Commission (2020). Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767, 20.1.2021.

European Commission (2020). White Paper on Artificial Intelligence - A European approach to excellence and trust, 19.2.2020, COM(2020) 65 final, retrieved from: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, 20.1.2021.

European Commission (2020). Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN, 20.1.2021.

European Commission (2020). Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final, retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN, 20.1.2021.

European Commission (2020). Shaping Europe's Digital Future, February 2020, retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/fs_20_278, 20.1.2021.

European Union (2012). Treaty on the Functioning of the European Union, consolidated version, OJ C 326, 26.10.2012, pp. 47–390.

European Union (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178, 17.7.2000, p. 1–16.

Federal Ministry for Economic Affairs and Energy (BMWi) (2019) Project GAIA-X—A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem, retrieved from: https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4, 20.1.2021.

Floridi L. (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, 33, pp. 369-378.

Gencor v. Commission, Judgment of the General Court, Case T-102/96, [1999] E.C.R. II-753.

Geradin D. and Reysen M. and Henry D. (2011) Extraterritoriality, Comity, and Cooperation in EU Competition Law. In A. Guzman (ed.) *Cooperation, Comity and Competition Policy*, Oxford: Oxford University Press, 2011.

Grosfillex-Fillistorf [1964] 3 CMLR 237.

Hackenbroich, J. (2020) China, America, and how Europe can deal with war by economic means. European Council on Foreign Relations, retrieved from https://ecfr.eu/article/commentary_china_america_and_how_europe_can_deal_with_war_by_economic_means/, 20.1.2021.

Imperial Chemical Industries Ltd. v. Commission of the European Communities (*Dyestuffs*), ECJ judgment, Case 48/69, [1972] E.C.R. 619.

In re Wood Pulp Cartel, 1985 O.J. (L 85) 1, [1985] 3 C.M.L.R 474 (1985).

Intel Corporation v European Commission, Case C-413/14 P, ECLI: EU: C: 2017:632.

Jobin A. and Ienca M. and Vayena E. (2019) The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, pp. 389-399.

Majstorović M. (2020). Opšta uredba Evropskog parlamenta i Saveta Evropske unije o zaštiti podataka (GDPR) – pregled i novine, *Evropsko Zakonodavstvo*, XIX (73-74), pp. 99-118.

Rahman T. (2020) Quantum Computing and Geopolitics. *Fintech*, retrieved from http://www.fintechbd.com/quantum-computing-and-geopolitics/, 20.1.2021.

Renda A. (2020). Artificial Intelligence: Towards a Pan-European Strategy. In: C. Hobbs (ed.), *Europe's digital sovereignty: From rule-maker to superpower in the age of US-China rivalry*, European Council on Foreign Relations, retrieved from https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/, 20.1.2021.

Shapiro J. (2020) Introduction: Europe's Digital Sovereignty, in C. Hobbs (ed.) *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*, European Council on Foreign Relations, 2020.

Tekir G. (2020) Huawei, 5G Network and Digital Geopolitics. *International Journal of Politics and Security*, 2(4), pp. 113-135.

Von Behr I. et al (2013) *Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism*. Washington D.C., Rand Corporation.

Vučić M. (2020) Granice vanteritorijalnog dejstva Opšte uredbe o zaštiti podataka Evropske unije. *Evropsko Zakonodavstvo*, XIX (73-74), pp. str. 41-60.