

A.R. Oralov
I.A. Maratov

L.N. Gumilyov Eurasian National University Astana, Kazakhstan
(E-mail: asylhan_pvl_95@mail.ru, Ilyas.com1999@gmail.com)

Main directions of the EU digital policy at the current stage

Abstract. *This article will analyze an EU digital policy and its cooperation with other countries. As we can see today, digitalization has a huge impact on every sphere of people's and state's lives, and its closely intertwined with the policy-making of the EU. The European Union works with partners around the world to advance its values and interests in many areas, including the digital sphere. This shows how a European approach can help others manage digital transformation in areas such as free data flow, human-centered artificial intelligence (AI), 5G, cybersecurity, privacy protection, data management etc. The path of digital space has been crossed by the process of European integration. In addition to being tied to information and communication technologies (ICTs) in the Union, «digital» is a keyword in the policies, speeches, and strategies of the European institutions that are tied to other categories of common policies of the Union, such as industry, the social dimension, research, or security. These indicators of the significance of digital policies in the Union include the fact that they are at the center of the public discourse in Europe and that they are horizontal, spanning multiple industries.*

The topic arises from the digitalization of the world and the EU is not trying to stay behind.

Keywords: *Digital policy, European Union, digitalization, foreign cooperation, digital sovereignty, data protection, personal data privacy, data governance.*

DOI: <https://doi.org/10.32523/2616-6887/2023-142-1-94-103>

Received: 10.08.2022/ Accepted: 12.01.2023

Introduction

Politicians, businesspeople, and members of civil society all now find it very vital to deliberate on issues related to technology and technological advancement. The social, political, educational, or cultural implications of information and communication technologies (ICTs) have been the subject of extensive discussion since these technologies left research labs and entered the lives of citizens.

The first observation to be made regarding the deployment of ICTs in society and the economy is clear according to science. They have the ability

to transform, and occasionally their results are regarded as revolutionary. The amount of their life-altering influence is still up for debate, nearly matching the globalization controversy.

The European Union's (EU) main aim is to create a «Europe fit for the digital age,» which is also essential to the EU's attempts to recover economically from the Coronavirus Disease 2019 (COVID-19) pandemic. The EU seeks to boost its economy and raise the region's digital competitiveness in comparison to the US and China under the «Shaping Europe's Digital Future» digital policy roadmap from the European Commission. The EU is pursuing

legislative, judicial, and administrative actions as part of its campaign to obtain what some EU leaders have dubbed «digital (or technological) sovereignty.» The different EU efforts included in the strategy span a wide range of topics, including data protection, competitiveness, and artificial intelligence (AI). Some American businesses have expressed concern that the new regulations would make it harder for them to compete in the EU market.

In the absence of a clear U.S. strategy or international accords, several officials and commentators argue that the EU's head start in creating digital standards may enable it to create global norms. Numerous EU initiatives are still in the proposal or draft stages, giving U.S. policymakers and other stakeholders time to offer their opinions. There may be prospects for U.S.-EU cooperation because parallel efforts are being made in the US to solve comparable technology concerns that the EU is focusing on. The United States and the European Union have similar fundamental democratic ideals and values, allowing for closer alignment or harmonization in some areas, notwithstanding the differences in their methodologies and risk tolerances. If they want to reach a consensus and act as a counterbalance to China's authoritarian approach in the digital sphere, U.S. and EU negotiators must find common ground. The US and EU should head a group of nations with similar ideologies centered on technology, according to numerous political figures and policy experts. As Congress considers legislation to alter or create new digital rules, it may take into account:

- (1) assessing the potential impact of the EU rules on the U.S. economy;
- (2) determining how EU policies may contrast or compare with U.S. policies;
- (3) conducting oversight on the domestic regulatory processes;
- (4) examining opportunities for global leadership on digital norms.

Congress may seek to work with the Biden Administration on trade or other initiatives to engage the EU on digital rules, including bilateral or multilateral efforts on these and other

technology concerns. At the same time, challenges persist to greater U.S.-EU cooperation. Different approaches, rules, and regulations in the digital realm and recent heightened tensions, and even distrust in the broader U.S.-EU relationship during the Trump Administration, contribute to these challenges. The Biden Administration has stated that it seeks to improve relationships with foreign partners, including the EU, and aims for greater international cooperation. It remains to be seen whether or how some key U.S.-EU differences can be bridged in the online sphere. This report provides an overview of selected EU digital initiatives; analyzes how EU policies may contrast with or be similar to U.S. policies, particularly in trade agreements; and examines issues of possible congressional interest, including the impact of such initiatives on U.S. firms and U.S. leadership in trade agreement negotiations and rule making on key technology issues.

Digital projects of the European Union

«A Europe fit for the digital age» is one of European Commission President Ursula von der Leyen's six main goals for the 2019–2024 term. She is in charge of the EU's executive arm [1; c.1]. The «Shaping Europe's Digital Future» digital policy roadmap from the European Commission outlines a number of projects that are anticipated to be at the center of the EU's digital agenda during the next years. The creation of a «fair and competitive» EU digital economy is the goal of measures being considered by the EU. Some of these projects expand on earlier efforts to unite the EU members through a Digital Single Market. These initiatives resulted in modifications like the General Data Protection Regulation (GDPR), which came into force in 2018 and established guidelines and requirements for personal data [2, p.16].

Several developments, including 5G, artificial intelligence (AI), cloud computing, and the internet of things (IoT), have become key strategic assets for the EU economy during the previous decade. With the global market for new digital technologies anticipated to reach €2.2 trillion by

2025, digital markets account for a significant portion of Europe's economic potential [3, p. 28].

While the EU has many strengths, such as a world-leading AI research community and a robust industry, certain data indicate that the EU also has key flaws that are harmful in the global competition to create such new technologies. In the field of artificial intelligence (AI), for example, the EU lags behind the United States (US) and China in terms of private investment, and the degree of adoption of AI technologies by businesses and the general public is low in comparison to the US. The United States also draws more AI talent and researchers and is the world leader in patent applications, although China leads the race in data gathering and access (i.e., the raw material for most AI technology) and has made tremendous progress in building AI and has made significant progress in the development of new hardware such as supercomputers [4, p. 1].

Digital sovereignty of the EU

The concept of «digital sovereignty» has lately developed as a strategy for fostering European leadership and strategic autonomy in the digital domain. Concerns have been made about the economic and social power of non-EU technology corporations, which affects EU individuals' sovereignty over their personal data and limits the expansion of EU high-tech enterprises as well as the ability of national and EU policymakers to enforce their laws [5, p. 27]. In this perspective, «digital sovereignty» refers to Europe's ability to operate freely in the digital world, and it should be interpreted in terms of both defensive measures and offensive capabilities to stimulate digital innovation that include collaboration with non-EU enterprises[6].

In this regard, Ursula von der Leyen, President of the European Commission, has designated digital policy as one of her top political goals for the 2019-2024 term and stated that Europe must attain «technical sovereignty» in vital sectors. According to a recent Commission assessment, competition from global tech-driven organizations that do not always follow

European regulations and core principles, and who place data appropriation and valuation at the center of their strategy, poses a huge policy issue for Europe. The European Parliament has voiced considerable worry about the security risks associated with China's rising technology presence in the EU and has urged for possible EU-level measures to decrease such reliance.

Similarly, the coronavirus epidemic that shook the EU in spring 2020 demonstrated the critical significance of the high-tech industry in maintaining the continuity of social life, enterprises, and governments, and has intensified debate on the necessity for sovereign digital technologies. In its recovery plan, the European Council called for measures to safeguard the EU's strategic autonomy in a post-pandemic scenario, emphasizing that investment in digital capacities, infrastructure, and technologies will be critical to the recovery effort.

For example, the suggested Digital Markets Act (DMA) would develop competition laws for large online platforms designated by the EU as «gatekeepers» [7]. The EU aims to establish a more equal regulatory environment for small and medium-sized firms (SMEs) or new entrants by addressing market concentration caused by the «network effect,» which makes online platforms more desirable as more users are added. Because user data is frequently required for participation with an online platform, EU officials caution that aggregation of such data might boost that platform's competitive position at the expense of SMEs or new market entrants. As a result, data collection and use, as well as traditional competition measurements, play an important part in evaluating market supremacy. Margrethe Vestager, Executive Vice President of the European Commission (in charge of EU digital policy), testified before the United States Congress on the need for new regulations and powerful enforcement measures to address the «severe harm to competition, innovation, and ultimately to consumers» caused by gatekeepers and their dual role as a platform operation and competitor in some markets [8].

In the DMA draft, the criteria for defining a «gatekeeper» include digital platforms with at

least 6.5 billion euros (approximately \$7.9 billion) in European revenue or a market capitalization of at least 65 billion euros (approximately \$79 billion), and serve more than 10,000 active business customers and 45 million active end users in the bloc (approximately 10% of EU consumers). Furthermore, any organizations that, first, operate in at least three EU countries, second, manage a digital environment that competitors use to access clients, and last but not least retain a dominant market position would be included, catching online intermediaries that dominate certain industries (e.g., online travel). The commission would be able to designate more organizations as gatekeepers after completing an inquiry, and companies would be able to challenge their designation at any moment.

The DMA proposal contains new *ex ante* guidelines for platforms, as well as a list of «do's and don'ts» for gatekeepers, outlining which services are permitted or forbidden. Platforms, for example, must enable business users to advertise their services and execute contracts with clients outside of the gatekeeper's platform and must not compete with those users using data gathered from those users. Another proposed rule would compel platforms to inform the commission of any planned acquisitions. Rules violations may result in fines of up to 10% of a company's total worldwide yearly sales. The commission may apply behavioral or structural sanctions in specific situations.

The commission also hopes to standardize online competition rules throughout the EU by the DMA, although the concept is still being debated. The draft legislation is still being reviewed by officials from the commission, Parliament, and member states. Some of them have emphasized the necessity for local governments to preserve flexibility in light of the *ex-ante* approach to laws and the automatic labeling of some corporations as gatekeepers. Some parties have expressed concern that the proposal lacks a defined market purpose or an impact assessment of the specific harm(s) addressed by the legislation.

A proposed new cooperation mechanism in the DSA between member state regulators would aim to improve enforcement and further

harmonization across the bloc. Fines would be imposable by a new EU-level body or by individual member states on entities in its jurisdiction. With no EU-wide definition of illegal content, it is unclear what the outcome would be if one member state requested that a platform based in another member state remove content that is legal in its home country.

Some big U.S. technology corporations are proactively building new transparency measures in the face of greater scrutiny and in anticipation of future regulation of online material, as well as to assist limit damage to their business model. Google, for example, announced the establishment of a new Google Safety Engineering Center in Ireland, which will serve as a «regional hub for Google experts working to combat the spread of illegal and harmful content, as well as a place where we can share this work with policymakers, researchers, and regulators»[9]. Facebook, for example, formed an Oversight Board to independently review and «make binding judgments on what content Facebook and Instagram should allow or remove, based on respect for free expression and human rights»[10, p.1].

Personal data privacy

The EU views communication privacy and personal data protection to be basic rights that are entrenched in EU law. Unlike the US, the EU has had an overarching data privacy protection legislation in place since 1995 with the Data Protection Directive (DPD). The EU's General Data Protection Regulation, which superseded the DPD on May 25, 2018, emphasizes some of the disparities between the US and EU approaches to data privacy[11, p.1-2]. The GDPR establishes common rules for data retention, storage limitation, and recordkeeping, as well as identifies legitimate bases for data processing. The extraterritorial character of the rule has repercussions for many U.S. corporations.

The GDPR develops a set of standards for the protection of personal data across the EU in order to increase individual rights and make business easier. The EU thinks that the GDPR would help

to further build the EU's Digital Single Market (DSM), which aims to increase digital policy harmonization throughout the union. The EU also sees the GDPR as supporting efforts to accelerate the EU's digital transformation and strengthen the EU's technology industry in comparison to Chinese and US rivals, all while defending European values.

The GDPR is used by all businesses and organizations with an EU establishment that process (i.e., perform operations on) personal data of EU individuals (or «data subjects»), regardless of where the actual processing of the data takes place; and entities outside the EU that offer goods or services (for payment or free) to EU individuals or monitor EU individual behavior. Certain sensitive personal data processing is typically forbidden. Noncompliance can result in a punishment of up to 4% of a company's annual worldwide revenue or €20 million [11, p. 1-2].

Many businesses in the United States have implemented modifications to comply with the GDPR, such as amending and clarifying user terms of agreement and requesting explicit authorization. While the GDPR imposes greater restrictions on organizations that collect or process data in the EU and the United States, some experts believe that the GDPR may ease compliance for U.S. corporations because the same set of data protection regulations applies across the EU. Furthermore, enterprises founded in the EU that participate in cross-border data processing must primarily communicate with the DPA of the EU nation in which the firm is headquartered (the «lead» authority), potentially lowering administrative expenses. A firm, however, is still subject to monitoring and enforcement. Some member countries and privacy campaigners have questioned the system since many of the major digital corporations are headquartered in a few countries and are monitored by the DPAs of those countries, resulting in enforcement delays and bottlenecks owing to limited resources [11, p. 1-2].

Several US companies have expressed worries about the GDPR, including the necessity to build a compliance bureaucracy and the possibility of

large expenses for conforming to the GDPR's obligations. While major corporations can afford consultants and attorneys, small and medium-sized organizations (SMEs) may find it more difficult and costly to comply, thereby discouraging them from accessing the EU market and establishing a de facto trade barrier. Some American companies, notably several newspaper websites and digital advertising agencies, chose to leave the EU market rather than deal with the intricacies of GDPR. According to several industry studies, GDPR's limits on data usage and sharing may be hindering the development of innovative technologies and preventing possible mergers and acquisitions.

GDPR and Data Flows Between the United States and the European Union:

To transport personal data beyond the EU, a company must comply with GDPR by transferring data (1) to a country deemed adequate for data protection by the EU, (2) via EU-approved standard contractual clauses (SCCs), or (3) via legally enforceable corporate standards. The European Court of Justice banned the US-EU Privacy Shield Framework as a method for data transfers in July 2020, raising concerns regarding the use of SCCs for US corporations vulnerable to US surveillance laws.

Data flow and regulation

Following a public consultation phase on an overall data and cloud services strategy, the European Commission announced its proposal for data regulation, the Data Governance Act, in November 2020 [12]. The commission's proposed strategy aims to establish «a new European approach of data governance that is consistent with EU values and principles,» as well as to give a trustworthy data-sharing alternative to «Big Tech» portals (e.g., U.S. tech companies like Google or Microsoft). The proposed rules settle the legal groundwork for an EU-wide single market for data sharing, with a focus on public and industrial, nonpersonal data, while also encouraging «data altruism» among EU citizens to share their personal data for «the common

good»; all data sharing by companies and individuals would be voluntary. According to the commission, the proposed additional measures might yield up to €7-11 billion in economic gains by 2028[12].

The proposed Act establishes responsibilities and norms for impartial «data intermediaries» to allow data exchange, as well as nine sectoral data spaces with diverse methods and requirements. Non-EU organizations might engage in data sharing if they met the EU conditions, which include having a presence in the EU. The measure would not oblige firms to retain data in the EU, assuaging non-EU organizations' initial concerns.

Data transfers beyond the EU might be restricted under the plan if a third country's data rules are deemed weak and not equal to EU requirements. The sharing of sensitive data with foreign national authorities, as well as the number of persons or corporations that can obtain and reuse the data, could be limited. Some stakeholders are concerned that the Data Governance Act will establish an adequate system for cross-border data flows that will necessitate a lengthy approval process for international data transfers or destination countries, similar to GDPR and that such a process will not be scalable on a global scale.

The Data Governance Act would be based on the Franco-German effort GAIA-X, a nonprofit organization aimed at creating a safe, federated platform for data infrastructure cloud service providers[13]. The non-profit organization attempts to promote common standards, regulatory frameworks, and policies in order to construct a safe, trustworthy network infrastructure and an ecosystem of cloud-service providers.

For European cloud service customers and businesses, an open, interoperable environment is essential. GAIA -X was created by 22 businesses and organizations (11 German and 11 French). It is open to everyone.

Companies from Europe and beyond the EU may join with restricted privileges. Amazon Web Services, Huawei, and IBM are among the major non-EU members.

Artificial Intelligence (AI)

In February 2020, the European Commission released a white paper for public comment on AI setting out policy options to promote AI and to regulate potential risks[14, c.1]. The white paper proposes categorizing certain AI applications as “high-risk” that would require ex-ante conformity assessment for market access while “non-high risk” AI applications would be subject to a voluntary labeling scheme. The EU seeks to ensure “trustworthy AI” building on the ethics guidelines identified by an EU expert panel.⁴⁵ In differentiating the EU strategy, officials and EU documents describe the need for a human-centric approach that aligns with EU norms. As the EU drafts its AI policy, a split is appearing between some member states, such as Germany, that prefer a strong regulatory approach and others, such as Denmark, that prefer self-regulation and voluntary practices along with standardization [14, p. 25].

In their responses to the white paper, U.S. stakeholders expressed concerns that new rules on AI could stifle innovation. Some of these stakeholders recommended instead that the EU adapt existing rules and promote “soft law” options such as industry-led standards and codes of conduct.

The fundamental components of a future legislative framework for AI in Europe that will generate a distinct «trust ecosystem.» To do so, it must assure compliance with EU legislation, especially those safeguarding basic rights and consumer rights, particularly for high-risk AI systems operating in the EU. Building a trust ecosystem is a policy goal in and of itself, since it should provide individuals the confidence to use AI apps and corporations and public organizations the legal certainty to innovate with AI. The Commission firmly favors a human-centric approach based on the Communication on Building Trust in Human-Centric AI⁸, and will also consider feedback received during the testing phase of the Ethics Guidelines developed by the High-Level Expert Group on AI.

The European data strategy that accompanies this White Paper intends to allow Europe to

become the world's most appealing, secure, and dynamic data-agile economy, empowering Europe with data to make choices and enhance the lives of all its inhabitants. The plan outlines a variety of policy initiatives, including the mobilization of private and governmental investments, that are required to attain this aim. Finally, the Commission Report that accompanies this White Paper examines the implications of AI, the Internet of Things, and other digital technologies for safety and liability regulation.

AI is a crucial technology that can help citizens, businesses, and society as a whole if it is human-centered, ethical, sustainable, and respects fundamental rights and values. AI provides significant efficiency and productivity improvements, which can boost European industry's competitiveness and increase residents' well-being. It may also help find solutions to some of society's most pressing problems, such as the fight against climate change and environmental degradation, the challenges associated with sustainability and demographic changes, the defense of our democracies, and, where necessary and proportionate, the fight against crime.

The United States and European Union cooperation

Since the United States and the EU share many of the same democratic, liberal norms and principles, as well as comparable digital concerns, several stakeholders have voiced excitement about future US-EU collaboration and collaborative leadership on digital and technological problems. Because of the Biden Administration's emphasis on international collaboration, as well as the EU's commitment to working in multilateral forums on these issues, particularly with the US, there is a chance for two of the world's major developed economies to collaborate. Several observers wonder how the two sides can overcome their contrasts in technology and science-based regulatory methods, given the US risk-based strategy and the EU's more risk-averse approach based on the «precautionary principle»[15]. Taking into

consideration these differences, some parties see opportunity for bilateral and international collaboration to develop and promote basic principles and norms for the digital world, even if total regulatory alignment or harmonization of the two systems is not possible.

For example, Organization for Economic Cooperation and Development (OECD). The Organization for Economic Cooperation and Development (OECD) is an intergovernmental organization that presents itself as «a unique platform and information center for data and analysis, exchange of experiences, best-practice sharing, and advise on public policies and international standard-setting» [16]. Meetings and working groups of the OECD create both binding and nonbinding guidelines, but the organization lacks an inherent enforcement mechanism and must rely on member adoption. Digital taxes is already the topic of OECD global discussions. The OECD is also a forum for debating new technology. Members are creating guidelines to meet the difficulties posed by emerging technologies and to build «fit for purpose» regulation where appropriate through the OECD Regulatory Policy Committee and the Network of Economic Regulators [17].

The U.S and the E.U have signed on to the OECD AI Principles, which aim to foster creative and trustworthy AI that respects human rights and democratic ideals[18]. The principles' goal is to provide «realistic and adaptable» norms that allow for growing technology while complementing other OECD standards on privacy, digital security risk management, and responsible corporate behavior. Furthermore, both the US and the EU are members of the Global Partnership on Artificial Intelligence (GPAI), which has formed working groups comprised of representatives from the public and business sectors, civil society organizations, and academics to address various issues of AI.

The OECD Privacy Guidelines of 1980 created the first worldwide set of privacy standards stressing data protection as a prerequisite for unrestricted cross-border movement of personal data [19]. The recommendations, which were updated in 2013, outline concepts for nations to consider when developing national policy,

with an emphasis on interoperability. 100 As with AI and privacy, the OECD may be a vehicle for developing shared standards and best practices on other digital challenges like content moderation and platform competition [19].

Conclusion

The EU's technology advances and anticipated new digital standards have far-reaching implications for US policymakers. The EU rules have the potential to have an economic impact on the United States by limiting the ability of US firms to conduct business in the EU or requiring those enterprises to make changes. Because of the timing of the EU proposals, US authorities may be unable to present an alternative model for developing global standards. At the same time, the EU initiatives might open the way for US-EU collaboration on mutually beneficial areas like digital commerce and technology.

Policymakers in the EU have begun to develop measures to increase the bloc's digital strategic autonomy. Several financial instruments have been implemented in recent years to close the investment gap, and additional measures to adapt the EU's industrial and technological capacities to the competitive environment are being considered in the context of the European data strategy and the AI ethical framework. The EU is becoming viewed as a leader in privacy and data protection, and it has already made significant legislative progress in cybersecurity

and 5G network security. Furthermore, guaranteeing openness and trust has become a hallmark of the EU's digital strategy. In light of this, recommendations have been made to push further measures at the EU level to speed the digitalization process, namely to construct a data foundation, establish a trustworthy digital environment, and adjust competition and regulatory norms. Fostering investment in ethical AI and frontier technologies, establishing public-private partnerships, and developing a large-scale EU research cooperation framework in the field of new technologies are all expected to boost the EU's innovation capability. Building a secure pan-European data architecture and implementing new standards and practices to deliver trustworthy and controlled digital products and services will result in a safer digital environment consistent with EU values and principles. Moreover, a change toward more defensive and prudential measures in the competitive and regulatory environment, including new regulations to address foreign state ownership and the distortive behaviors of giant tech corporations, is needed in order to attain greater technical autonomy. If new bilateral forums or agreements are to be explored, Congress may establish explicit guidelines to establish priorities or limitations. Congress may discuss how authorities in the United States and the European Union might overcome the obstacles that have previously hampered increased US-EU collaboration.

References

1. European Commission, Directorate-General for Communication, Luyen, U., A Union that strives for more : my agenda for Europe : political guidelines for the next European Commission 2019-2024, Publications Office. [Web resource]. – 2022. – URL: <https://data.europa.eu/doi/10.2775/018127> (accessed 01.06.2022).
2. For more information on the EU's Digital Single market strategy 2014-2019, see European Commission, "Shaping the Digital Single Market," October 29, 2020, <https://digital-strategy.ec.europa.eu/en/library/shaping-digital-transformation-europe>. -internet resource(accessed 04.11.2022).
3. Castro D., McLaughlin M., Chivot E., August 2019. Who Is Winning the AI Race: China, the EU or the United States? . [Web resource]. – 2022. – URL: datainnovation.org (accessed 01.06.2022).
4. Castro D., McLaughlin M., Chivot E., August 2019. Who Is Winning the AI Race: China, the EU or the United States? . [Web resource]. – 2022. – URL: datainnovation.org (accessed 01.06.2022).
5. ESPAS. [Web resource]. – 2022. – URL: <https://www.fondapol.org/app/uploads/2020/06/f-gueham-digital-sovereignty-3.pdf>.- internet resource (accessed 09.11.2022).

6. European Commission. January 2018. Advanced Technologies for Industry (europa.eu). Tyson Barker. January 16, 2020. "Foreign policy" html/: Europe Can't Win Its War for Technology Sovereignty. [Web resource]. – 2022. – URL: foreignpolicy.com. (accessed 02.12.2022).
7. European Commission, "The Digital Markets Act: ensuring fair and open digital markets," November 2022. [Web resource]. – 2022. – URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en. (accessed 02.11.2022)
8. U.S. Congress, House Committee on the Judiciary, Subcommittee on Antitrust, Commercial, and Administrative Law, Online Platforms and Market Power, Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google, 116th Cong., July 29, 2020. (accessed 04.12.2022)
9. For more information on the EU's Digital Single market strategy 2014-2019, see European Commission, "Shaping the Digital Single Market," October 29, 2020, [Web resource]. – 2022. – URL: <https://digital-strategy.ec.europa.eu/en/library/shaping-digital-transformation-europe>. (accessed 04.11.2022).
10. Klonick, Kate, The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression (June 30, 2020). Yale Law Journal, Vol. 129, No. 2418, 2020, Available at https://scholarship.law.stjohns.edu/faculty_publications/312/ (accessed 04.11.2022).
11. Rachel F. Fefer , Kristin Archic. July 17, 2020. EU Data Protection Rules and U.S. Implications. [Web resource]. – 2022. – URL: fas.org. (accessed 09.11.2022).
12. Data Governance Act. November 25, 2020 . [Web resource]. – 2022. – URL: EUR-Lex - 52020PC0767 - EN - EUR-Lex (europa.eu). (accessed 01.06.2022).
13. GAIA-X. October,2019. GAIA-X. [Web resource]. – 2022. – URL: data-infrastructure.eu. (accessed 04.11.2022).
14. WHITE PAPER On Artificial Intelligence. February 19,2020. - A European approach to excellence and trust. [Web resource]. – 2022. – URL: commission-white-paper-artificial-intelligence-feb2020_en.pdf (europa.eu). (accessed 04.12.2022).
15. CRS reports. March 25, 2021. CRS Search Results. [Web resource]. – 2022. – URL: congress.gov. (accessed 01.06.2022).
16. The Organisation for Economic Co-operation and Development (OECD), About the OECD - OECD. [Web resource]. – 2022. – URL:<https://www.oecd.org/about/>. (accessed 02.12.2022)
17. OECD Regulation policy. October 4,2022. Regulatory policy 2.0. Viewpoints and beliefs about better regulation: A report from the "Q exercise" | OECD Regulatory Policy Working Papers | OECD iLibrary. [Web resource]. – 2022. – URL:oecd-ilibrary.org. (accessed 02.12.2022).
18. OECD principles on AI. February 22,2022. Artificial intelligence - OECD, also OECD Framework for the Classification of AI Systems: a tool for effective AI policies. [Web resource]. – 2022. – URL: OECD.AI. (accessed 06.11.2022).
19. The Organisation for Economic Co-operation and Development (OECD). [Web resource]. – 2022. – URL: <https://www.oecd.org/>. (accessed 06.11.2022).

А.Р. Оралов, И.А. Маратов

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

ЕО-тың қазіргі кезеңдегі цифрлық саясатының басты бағыттары

Аңдатпа. Бұл мақалада ЕО-ның цифрлық саясаты және оның басқа елдермен ынтымақтастығы талданады. Бүгінгі таңда көріп отырғанымыздай, цифрландыру адамдар мен мемлекет өмірінің барлық салаларына үлкен әсер етеді және ол ЕО саясатының қалыптасуымен тығыз байланысты. Еуропалық Одақ өзінің құндылықтары мен мүдделерін көптеген салаларда, соның ішінде цифрлық салада ілгерілету үшін бүкіл әлемдегі серіктестермен ынтымақтасады. Бұл еуропалық тәсіл басқаларға цифрлық трансформацияны басқаруға қалай көмектесе алатынын көрсетеді, мысалы, еркін деректер ағыны, адамға бағытталған жасанды интеллект (AI), 5G, киберқауіпсіздік, құпиялылықты қорғау, деректерді басқару және т.б. сандық кеңістік жолы еуропалық интеграция процесімен қиылысқан. Одақтағы ақпараттық-коммуникациялық технологиялармен (акт) байланыстырудан басқа, «цифрлық» - бұл өнеркәсіп, әлеуметтік

өлшем, зерттеу немесе қауіпсіздік сияқты Одақтың жалпы саясатының басқа категорияларымен байланысты Еуропалық институттардың саясатындағы, сөйлеген сөздеріндегі және стратегияларындағы кілт сөз. Одақтағы цифрлық саясаттың маңыздылығының бұл көрсеткіштеріне олардың Еуропадағы қоғамдық талқылаудың орталығында екендігі және көптеген салаларды қамтитын көлденең сипатқа ие екендігі жатады.

Бұл тақырып әлемді цифрландыруға байланысты туындайды және ЕО шетте қалуға тырыспайды.

Түйін сөздер: Цифрлық саясат, Еуропалық Одақ, цифрландыру, шетелдік ынтымақтастық, цифрлық егемендік, деректерді қорғау, дербес деректердің құпиялылығы, деректерді басқару.

А.Р. Оралов, И.А. Маратов

Евразийский национальный университет им. Л.Н. Гумилева Астана, Казахстан

Основные направления цифровой политики ЕС на современном этапе

Аннотация. В этой статье будет проанализирована цифровая политика ЕС и его сотрудничество с другими странами. Как мы можем видеть сегодня, цифровизация оказывает огромное влияние на все сферы жизни людей и государства, и она тесно переплетена с формированием политики ЕС. Европейский союз сотрудничает с партнерами по всему миру для продвижения своих ценностей и интересов во многих областях, включая цифровую сферу. Это показывает, как европейский подход может помочь другим управлять цифровой трансформацией в таких областях, как свободный поток данных, ориентированный на человека искусственный интеллект (ИИ), 5G, кибербезопасность, защита конфиденциальности, управление данными и т.д. Путь цифрового пространства был пересечен процессом европейской интеграции. Помимо привязки к информационно-коммуникационным технологиям (ИКТ) в Союзе, «цифровой» является ключевым словом в политике, выступлениях и стратегиях европейских институтов, которые связаны с другими категориями общей политики Союза, такими как промышленность, социальное измерение, исследования или безопасность. Эти показатели значимости цифровой политики в Союзе включают тот факт, что они находятся в центре общественного обсуждения в Европе и что они носят горизонтальный характер, охватывая множество отраслей.

Эта тема возникает в связи с цифровизацией мира, и ЕС не пытается оставаться в стороне.

Ключевые слова: Цифровая политика, Европейский союз, цифровизация, зарубежное сотрудничество, цифровой суверенитет, защита данных, конфиденциальность персональных данных, управление данными.

Information about the authors:

Oralov Assylkhan Razdykovich – Ph.D. student, Department of Regional Studies, Faculty of International Relations, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

Maratov Ilyas – Master student, Department of Regional Studies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

Оралов Асылхан Раздықұлы – саясаттану кафедрасының докторанты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Маратов Ильяс – Аймақтану кафедрасының магистранты, Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан