International Organisations Research Journal, 2022, vol. 17, no 1, pp. 96–113
Original Article
doi:10.17323/1996-7845-2022-01-04

The Influence of the G20's Digitalization Leadership on Development Conditions and Governance of the Digital Economy[1]

A. Shelepov

Andrey Shelepov – Candidate of Economic Sciences, Senior Researcher, Centre for International Institutions Research, Russian Presidential Academy of National Economy and Public Administration; 11 Prechistenskaya naberezhnaya, 119034, Moscow, Russian Federation; shelepov-av@ranepa.ru

Abstract

Given the increasing importance of the digital economy, competition for digital technologies and solutions, as well as the contest to influence norms, standards, and regulatory mechanisms, is escalating. This influence is distributed unevenly – digitalization leaders, primarily the key Group of 20 (G20) members, gain significant advantages, increasing their potential for shaping digital regulation through the consistent inclusion of domestic standards and norms in the documents of multilateral institutions, including the G20, the Organisation for Economic Co-operation and Development (OECD), the World Trade Organization (WTO), and the United Nations (UN). At the same time, Russia's impact on the most important aspects of digital economy regulation at the global and regional level is currently limited.

The article presents an assessment of the influence wielded by the leading G20 members (the U.S., Canada, the UK, the European Union (EU), Japan, Korea, China and India) on the digital economy's development and regulation. This assessment serves as the basis for recommendations on Russia's approaches to the specific aspects of regulation (digital infrastructure development, cybersecurity, regulating digital platforms, regulating global stablecoins and central bank digital currencies (CBDCs), data governance, and artificial intelligence (AI) policies at the national level, as well as its engagement in the G20 and other multilateral institutions.

The analysis indicates that the leading countries affect the digital economy mainly by determining conditions for activities in their domestic digital markets and participating in shaping new global standards and rules. In the areas of digital infrastructure development, cybersecurity, and data governance, there are growing contradictions between the approaches of the U.S., the UK, Japan and partly the EU and Korea on the one hand, and Russia, China and India on the other. Recommendations in these areas are related to strengthening coordination within the BRICS group of Brazil, Russia, India, China and South Africa to develop common positions and collectively promote them in the G20 and other multilateral institutions. The main recommendations on other regulatory aspects include using the experience of digitalization leaders to minimize the risks posed by competitors and to strengthen Russian positions in the global digital economy.

Keywords: digital economy, G20, cybersecurity, digital platforms, central bank digital currencies (CBDC), data governance, artificial intelligence (AI)

Acknowledgments: the article was written on the basis of the RANEPA state assignment research programme.

For citation: Shelepov A. (2022) The Influence of the G20's Digitalization Leadership on Development Conditions and Governance of the Digital Economy. *International Organisations Research Journal*, vol. 17, no 1, pp. 96–113 (in English). doi:10.17323/1996-7845-2022-01-04

[1] This article was submitted 03.02.2022.

Introduction

Given the growing role of the digital economy in overcoming the COVID-19 pandemic and stimulating economic growth following the related crisis, competition for digital technologies and solutions is intensifying. At the same time, the contest to influence the regulation of the digital economy and the conditions for its development in various areas is escalating. The outcome of this competition for digital dominance and cooperation for digital equality will determine the balance of power in the future economic order.

Russia does not yet have a significant impact on the most important aspects of the regulation of the digital economy, such as cross-border data flows, ensuring privacy and protecting consumer rights, providing critical digital infrastructure security, developing and using artificial intelligence (AI), and regulating digital markets. At the same time, the leading developed countries are enhancing their potential to regulate the digital economy, including through the consistent inclusion of domestic standards and cooperation norms in the documents of multilateral institutions such as the Group of 20 (G20), the World Trade Organization (WTO), and the United Nations (UN) in order to create a global market based on their own approaches, thus providing additional opportunities for their technology companies, products, and services in this market. In this regard, this article assesses the leading G20 members' impact on the development conditions and regulation of the digital economy and makes recommendations for Russia's regulatory policies at the national level, as well as for its engagement with the G20 and other multilateral institutions.

To this end, a sample of leading digital economies was formed, including the UK, the U.S., Canada, the European Union (EU), Japan, Korea, India and China. These economies were included in the sample based on an expert assessment of the impact potential (in particular, of the Group of 7 (G7) and BRICS countries (Brazil, Russia, India, China and South Africa) as these economies can coordinate their positions and promote them collectively in more representative institutions) and data from international digital economy development ratings (Table 1). Both rankings with distribution by positions and ratings without direct comparison of examined countries were considered – for example, in the Organisation for Economic Cooperation and Development (OECD) Going Digital Toolkit ranking, the UK, the U.S. and Canada leave other countries behind in terms of most indicators. The EU, which is actively strengthening its potential for digital economy regulation at the supranational and international level, is considered as a substitute for individual European countries.

Table 1. Positions of the Selected Economies in International Digital Economy Development Ratings and Rankings

	U.S.	**Canada**	**EU (Germany)**	**UK**	**Japan**	**Korea**	**India**	**China**	**Russia**
International Telecommunication Union (ITU) Information and Communication Technology (ICT) Development Index	16	29	12	5	10	2	134	80	45
World Bank Group (WBG) Digital Adoption Index	27	36	6	23	8	4	92	74	28
World Economic Forum (WEF) Network Readiness Index	4	11	8	10	16	12	67	29	43

	U.S.	Canada	EU (Germany)	UK	Japan	Korea	India	China	Russia
Institute for Management Development (IMD) World Digital Competitiveness Ranking	1	13	18	14	28	12	46	15	42
UN E-Government Development Index	9	28	25	7	14	2	100	45	36
ICT sector share in gross domestic product (GDP) (%)	5.0	3.4	3.8	4.1	5.7	8.4	5.1	4.8	2.2
Global position in terms of the absolute size of the ICT sector	1	11–20	3 (EU)	7	4	5	6	2	11–20

Source: Compiled by the authors based on the data of the respective ratings and rankings.

The article considers the influence mechanisms that provide opportunities for promoting regulatory approaches through multilateral institutions for each of the selected countries and the EU in six priority areas: digital infrastructure development; ensuring cybersecurity; regulating digital platforms; regulating global stablecoins and central bank digital currencies (CBDCs); governing data flows; and AI policies.

Influence of Leading Countries on the Development Conditions and Regulation of the Digital Economy, and Recommendations for Russia

Global Leadership Pursuit as a Basis of Influence

It is important to note that most countries in the sample explicitly set global digital leadership goals in their policy documents. For instance, in 2021, UK authorities formulated the objective of ensuring the competitiveness of the national economy as a global digitalization and data hub in the context of geo-economic and geopolitical shifts, systemic competition, rapid technological changes, transnational challenges, and the ongoing impacts of the COVID-19 pandemic [Gov.UK, 2021a]. The U.S. National Cyber Strategy stressed that "the United States' influence in cyberspace is linked to... technological leadership" [President of the United States of America, 2018]. The EU is striving for global leadership in digital economy regulation, while Japan and Korea are taking systematic measures to maintain their leadership in the field of digital technologies. The strategic plans of the People's Republic of China (PRC) also provide for the transformation of the country into a global cyber power, leading the world in the main areas of digitalization and capable of influencing international digital standards. To achieve these goals, these countries actively use trade and investment policies, development assistance, participation in the activities of standard-setting organizations (for example, the International Organization for Standardization (ISO) and the ITU) and other international institutions. Countries such as India and Canada do not explicitly set goals for international leadership in their strategic documents, although they do prioritize internal digital development objectives. Accordingly, their degree of influence on global digital economy regulation is relatively lower.

Nevertheless, their approaches should also be taken into account by Russia when it implements bilateral cooperation projects and develops its own regulation.

Digital Infrastructure Development

Digital infrastructure development is a priority for all countries under consideration. The deployment of 5G infrastructure (in the EU, 6G as well) is carried out mainly using public resources and through the creation of incentives for business investment, as well as the implementation of secondary and shared frequencies and the free use of radio frequencies in accordance with ITU recommendations. This approach is typical for the U.S., the UK, Korea and Japan. Their experience may be relevant for Russia; however, the frequency range of 3.4–3.8 GHz that is considered the most convenient for commercial use of 5G networks is, in Russia, used by law enforcement and defence institutions, thus creating technical obstacles to the development of new technologies [TASS, 2021].

The objectives of overcoming the digital divide are relevant not only for countries where this problem is traditionally acute, such as India, but also for developed ones. For instance, the new U.S. administration emphasized the need to bridge the digital divide, given that about 30 million U.S. citizens do not have access to broadband networks, and that there are ethnic and racial disparities in the provision of high-quality Internet connectivity [The White House, 2021]. The importance of digital infrastructure development increased even more during the COVID-19 pandemic, as evidenced by the approval of new projects and the allocation of additional resources by all countries considered.

Given the growing competition, the approach of developed countries to digital infrastructure is to seek cooperation with like-minded states while limiting competitors' potential. For example, the UK Telecommunications (Security) Act of November 2021 tightened security requirements for telecoms and network providers and strengthened the powers of the Ofcom, giving it new decision-making powers in relation to high-risk vendors [Gov.UK, 2020]. In fact, according to the UK's official position, Chinese companies are included in this group. Additionally, most G7 countries have set the objective of enhancing their influence on the development of global telecom standards, including through increasing the number of representatives in international standard-setting institutions and the intensity of their work, strengthening strategic coordination between national actors (including business, governments and regulators) to ensure consistent positions in international institutions, and building strategic unity with partners, including a consensus on the need to provide interoperable telecom standards.

The most significant risk for Russia in this regard is the EU policy of extending influence on its neighbouring states, including within the framework of the Eastern Partnership. The main instrument of such influence is the EU4Digital programme (2019–22). The programme aims "to extend the European Union's Digital Single Market to the Eastern Partner states.... Through the initiative, the EU supports the reduction of roaming tariffs, the development of high-speed broadband to boost economies and expand e-services, coordinated cyber security and the harmonization of digital frameworks across society, in areas ranging from logistics to health, enhanced skills and the creation of jobs in the digital industry" [EU Neighbours East, n.d.]. The EU's policy affects, inter alia, Russia's strategic partners in the region, including the Eurasian Economic Union (EAEU) states.

China's Digital Silk Road initiative pursues similar goals [Shen, 2018]. The Digital Silk Road covers a range of projects related to infrastructure, e-commerce, research cooperation, and the promotion of Chinese standards and norms. Implementation of this initiative leads to strengthening China's global position, promoting Chinese standards, and increasing dependence of the countries engaged in this initiative on Chinese digital infrastructure. The Digital

Silk Road and other international projects of the PRC largely affect countries neighbouring Russia, including the EAEU members, thus complicating competition for Russian digital infrastructure suppliers and increasing the overall economic dependence of these countries on China. However, in contrast to the EU's policy, the Chinese initiative also has a positive impact associated with potential joint projects, such as the interface of GLONASS and Baidu satellite navigation systems and the development of 5G infrastructure.

Thus, in the area of digital infrastructure development, Russia could strengthen cooperation with China, taking into account the EAEU's digital agenda and the Digital Silk Road as an integral part of building synergies between the EAEU and the One Belt One Road (OBOR) initiative. It could also intensify cooperation with partners in the framework of Eurasian integration on harmonizing standards, establishing institutional and legal frameworks for the EAEU's digital agenda until 2025, and financing measures to bridge the digital divide both within countries (including the Russian Federation itself) and between them, thus limiting the EU's influence in the region.

Cybersecurity

The creation of a new digital infrastructure is closely related to security and competition issues. Ensuring cybersecurity, along with infrastructure development, is a priority in terms of digital economy financing for countries claiming the status of cyber power. For example, in 2016–20, the UK committed £1.9 billion to implement the National Cyber Security Strategy [NAO, 2021]. China aims to create a $40 billion market for cybersecurity products and services by 2023 [Xiong, Zhang, 2021]. Although both the UK and China strive to become leading cyber powers, their approaches to reaching this objective and identifying the main threats to it differ. The same is true for differences in general approaches to digital economy regulation between the developed countries, on the one hand, and India and China, on the other. The UK aims to establish strategic superiority through strengthening its science and technology sector and consolidating its position as the world's leading democratic cyber power. In this regard, the UK pays much attention to cyber threats emanating from other states, as well as response measures, including the expansion of sovereign capabilities to implement offensive cyber operations [Gov. UK, 2016]. The EU also strives to set global cybersecurity standards. European countries seek to prepare against potential cyberattacks by other states, including Russia. The EU builds cooperation either on its own terms (for instance, in the Organization for Security and Co-operation in Europe (OSCE)) or through institutions where Russia is not represented (the North Atlantic Treaty Organization (NATO), the OECD). There is a growing risk of spreading the EU's approaches and values, which in recent years have been increasingly at odds with Russian ones, and of losing opportunities to affect international decision-making. Unlike the EU, the UK, and other developed countries, China set the goal of sovereignty over key and critical technologies without striving for the global expansion of its standards [Government of the PRC, 2016]. This position is much closer to the Russian one.

G7 countries' attempts to promote a multilateral approach to Internet governance and multilateral cooperation models in international organizations, as opposed to countries with an alternative vision of the state-controlled Internet and reproduction of national borders in cyberspace, reflect the aspiration to consolidate their advantages in the existing digital governance system and contradict Russia's position on the need to guarantee all states equal rights and opportunities to participate in Internet governance [Ministry of Foreign Affairs of the RF]. Moreover, Russia, along with China, is directly mentioned in the G7 countries' documents on cybersecurity as a state that poses substantial threats [Gov.UK, 2021b]. Thus, the promotion of

G7 countries' values, norms and rules as a global standard through international institutions is a direct challenge for Russia.

In the context of a growing divergence of interests and values with the UK, the EU, the U.S. and Japan, and given their endeavour to set global cybersecurity standards, it is important for Russia, in addition to implementing domestic measures in accordance with the National Security Strategy, to facilitate multilateral discussion of relevant issues within influential fora such as the UN and the G20, to cooperate within the BRICS to agree on and promote the consolidated positions of the five countries (despite some contradictions between India and China), to strive to strengthen meaningful cooperation on cybersecurity in the Shanghai Cooperation Organization (SCO), and to promote confidence-building measures between countries in the cybersphere.

Regulating Digital Platforms

The growth of active digital platforms draws the attention of regulators in all the examined countries and the EU. In general, regulation in this area is aimed at protecting the interests of local suppliers and consumers and limiting large players' influence. The U.S. and China, in addition to this goal, try to prevent foreign platforms from entering their national markets. Although not always explicitly stated in the regulatory documents, this issue is considered a matter of national security. At the same time, regulation in these two countries is largely aimed at national digital platforms, as their active development could undermine free competition.

The dominant approach to regulating digital platforms is illustrated by the EU example. The European Union strives to limit the dominant position of the largest companies implementing the two main regulatory documents – the Digital Services Act (DSA) and the Digital Markets Act (DMA). The EU needs proper regulation of digital services, markets and platforms in order to control the activities of companies that are not formally located in the EU and are not subject to its law but which actively collect and process its citizens' data, provide services to them, and generally benefit from European clients and consumers. The DSA introduces a distinction between online intermediaries by singling out the category of "very large platforms," defined as having more than 45 million users, or 10% of the EU's population. Companies falling into this category will face additional rules regarding content moderation and targeted advertising [EC, 2020b]. The main burden of the new requirements falls on the largest global players, classified as "gatekeepers" in accordance with the DMA [EC, 2020c]. As a result, EU policy seems to be non-discriminatory toward small platforms while imposing strong oversight and accountability requirements on the largest companies.

Given the cross-border nature of technology companies' activities, leading developed countries are strengthening cooperation in their regulation, including through the Multilateral Mutual Assistance and Cooperation Framework, as well as the G7, the OECD, the International Competition Network (ICN), and the International Consumer Protection and Enforcement Network (ICPEN). In contrast to the two areas discussed above, common interests can contribute to developing coherent regulation of digital platforms at the international level and have a positive effect on regulating platforms in Russia. There are some examples of effective collective approaches to digital economy regulation. For instance, the decision to reform international tax rules in the digital economy agreed by the members of the OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting (BEPS) provided for the redistribution of rights to tax excess profits of the largest multinational enterprises (MNEs) (20–30% of profits received above the established threshold) in favour of jurisdictions where market activities are carried out and introduced a 15% minimum global tax for MNEs [OECD, 2021a].

Overall, there is an undoubted potential for a positive dialogue using foreign experience in regulating large digital platforms. For instance, the emerging EU scheme, with strict consumer protection rules, limits on the ability to use a dominant position in the market, and taxation of digital presence, or the UK regulation that provides for determining the strategic market status of companies, adopting codes of conduct, carrying out targeted interventions, implementing stricter mergers and acquisitions (M&A) regimes in relation to such companies, monitoring and requesting information, imposing fines, and making court decisions [Gov.UK, 2021c], can be considered as functionally close, although alternative, in terms of their implementation mechanisms, to the requirement of physical establishments in Russia. Given the commonality of approaches and the cross-border nature of digital companies' activities, it is important for Russia to integrate issues related to regulation of digital platforms into the BRICS and G20 digital economy agendas.

Regulating Global Stablecoins and Central Bank Digital Currencies

The goals of the central banks and finance ministries of Russia and the selected countries regarding the regulation of global stablecoins and issuance of central bank digital currencies (CBDCs) are quite similar. Given the inevitable, rapid emergence of global stablecoins, developing international regulation, monitoring, and supervision in this area is necessary to effectively use their advantages and minimize relevant risks. It may also have positive effects for Russia, although the central bank does not plan to allow the use of such currencies so far. As for issuing and regulating CBDCs, the development of common approaches in the Financial Stability Board (FSB), the Bank for International Settlements (BIS), the Committee on Payments and Market Infrastructures (CPMI), the International Monetary Fund (IMF) and the G20 could also be positive, especially given the Russian central bank's active engagement in testing the digital rouble [Bank of Russia, 2021], which could potentially make Russia one of the global leaders in this area.

There are some differences in country-specific approaches to achieving the goals of regulating digital financial assets [Shelepov, 2021]. The approaches of the considered jurisdictions to global stablecoins can be divided into two groups: the preventive development of regulation taking into account the expected rapid spread of global stablecoins and aimed at using their advantages and minimizing risks, on the one hand, and introducing restrictive measures, typical of countries with the potential for large-scale use of their own national digital currencies, on the another. The first approach is typical of most developed countries, and the second is implemented, for instance, in China [Ledger Insights, 2021]. An example of the first approach is the EU strategy [EC, 2020a] designed to utilize the potential of digital assets while reducing risks for investors and to financial stability. European regulation is aimed at ensuring legal certainty for all crypto assets, whether they qualify as financial instruments or electronic money under the current legislation or have not previously been regulated. The Markets in Crypto-Assets (MICA) regulation covers all such assets not currently subject to existing financial services legislation, including global stablecoins. Further, it covers the full range of legal persons engaged in the crypto assets services market, such as providers, exchanges, trading platforms and issuers. Crypto asset service providers will need to have a physical establishment in the EU and obtain prior authorization from the national competent authority before starting their activities. They will be subject to capital requirements, management standards, and an obligation to separate their clients' funds from their own assets. Crypto asset providers will also be subject to stringent cybersecurity requirements. Compliance will be monitored by national competent authorities or the European Banking Authority. Additional requirements for issuers of global stablecoins

include the obligation to be officially registered, as well as good governance and stabilization mechanism disclosure requirements, conflict of interest guidelines, and investment rules.

As for CBDCs, they have not yet actively spread in the selected countries and the EU. Of all these jurisdictions, only China has made significant progress in developing its CBDC, creating conditions for its rapid launch throughout the country if the authorities decide to do so [King, 2021]. The experience of countries with different approaches is relevant for Russia since its national regulation in the area is still being developed. At the same time, negative risks from other countries' influence are currently minimal.

To reap the benefits of new financial technologies and take a more significant place in the emerging system of cross-border payments based on digital currencies, Russia should intensify the work related to the G20 road map for enhancing cross-border payments and CBDCs in international institutions. So far, the G7 retains leadership in these areas; BRICS cooperation is stalling despite the stated goals of reforming the international monetary system and increasing the share of settlements in national currencies. As part of the national regulation development, the EU's experience can again be useful as its approach to the use of crypto assets does not provide for their full prohibition but maintains a high degree of control over issuers.

Data Flow Governance

As for data flow governance, growing inter-country contradictions are obvious, illustrated by the declaration of the goals of free cross-border data flows, primarily by developed countries, along with the simultaneous adoption of restrictive measures to protect data and critical information and preserve the competitive advantages of national companies. Data protection is the most regulated area among those considered. Appropriate laws have been adopted in almost all selected countries. In India, the Personal Data Protection Bill is being considered by a parliamentary committee [Dalmia, 2021]. In China, a draft law on the protection of personal information is under public discussion [WilmerHale, 2021].

Similar to their approach to cybersecurity, the selected developed countries promote a multilateral approach to data governance based on international regimes providing for interoperability of standards, consistency of legislation and cooperation between relevant national authorities. This creates opportunities for their "companies to work without additional barriers in their respective markets and internationalise and benefit from operating on a global scale" [OECD, 2021b, p. 4]. However, differences in approaches [Goodman, 2021] and problems of trust are evident not only between the bloc of like-minded developed countries and other states, including Russia and China, but also within this bloc [Swire, 2021], as illustrated by the Japanese presidency's "data free flow with trust" initiative that is stalling in the G20.

Nevertheless, there is a significant strategic unity among developed countries, which is facilitated, among other things, by more than 40 years of cooperation in protecting privacy and cross-border data flows in the OECD.[2] In most cases (in particular, in the EU, the UK and the U.S.) this regulation is extraterritorial, as it defines general requirements for all companies that collect or process data from citizens, regardless of their location, conditioning cross-border data transfer by adequacy decisions, appropriate safeguards, or mandatory corporate rules. In some cases, data transfer is regulated by bilateral agreements, such as the EU-U.S. Privacy Shield [Privacy Shield, n.d.]. At the same time, Russia, like the other BRICS members, applies localization requirements [Cory, Dascoli, 2021]. The Russian Federal Law No 152 that establishes

[2] The 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data became the first internationally agreed document in this area and has had a significant impact on the OECD members' policies.

this requirement is not extraterritorial, does not cover non-residents, and does not prohibit the transfer of Russian citizens' data. According to Article 12 of this law, personal data are transferred within the territories of states that are parties to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and, for transfer to the territories of countries that are not parties to the convention, an adequacy decision is required to ensure proper protection of personal data subjects' rights.[3] Nevertheless, foreign experts often consider the BRICS countries' legislation as protectionist, justifying calls for shaping international data governance without Russia and China and with digital authoritarianism and high data restriction indices [Ibid.].

The aspiration of G7 governments to establish a global data governance system based on shared values and to manage the "malicious" influence of rivals (including Russia and China) enhances risks associated with Russia being considered an outcast in this system with negative consequences for Russian companies and citizens. In this regard, it is important to increase the activity and quality of Russia's engagement in the dialogue on regulating data flows, including in the G20, and to strengthen the work on achieving a multilateral consensus within the framework of the WTO negotiation process in order to determine international standards for cross-border data transfer.

AI

Promotion of AI technologies is a cross-cutting priority affecting all digital development areas. The UK [Gov.UK, 2019], Korea [Government of the Republic of Korea, 2019], Canada [CIFAR, n.d.], China [Government of the PRC, 2017] and Russia [President of the RF, 2019] are implementing strategic programmes and plans in the AI sphere.

Despite the high perceived level of Russian developments in the field of AI and the 2019 forecast for the growth of AI's share in Russia's GDP to 0.8% in 2024 and 3.6% in 2030 [Government of the RF, 2019], the share of the Russian Federation in the global AI market is negligible. The National Strategy for the Development of Artificial Intelligence Until 2030 does not provide for measures to enhance Russia's participation in international cooperation on AI or develop regional and global partnerships, while the Federal Project "Artificial Intelligence" does not provide for relevant funding. Without appropriate support from the government aimed, inter alia, at promoting cooperation with the Global Partnership for AI, it will be challenging for Russian actors in this emerging international system to gain influence in standard- and norm-setting or to take any significant market share.

It is also important to consolidate positions on the potential engagement with the Global Partnership for Artificial Intelligence. This institution is one of the new initiatives to promote responsible AI development and use. An important feature of the partnership, distinguishing it from similar institutions operating as non-governmental organizations (NGOs), is its intergovernmental nature. The partnership was established in 2020 with the participation of the G7 countries, Australia, the EU, Mexico, New Zealand, Korea, Singapore and India. Despite political disagreements with most of these countries, Russia largely shares their positions regarding practical cooperation on AI. Partnership activities are mostly based on the OECD Recommendations on AI [OECD, 2019], which, in fact, are supported by Russia, since the G20 adopted AI principles with almost identical wording. Currently, the activities of the partnership are not aimed at unifying approaches to regulation as it mainly facilitates research cooperation and applied AI developments. However, in the future it may become a platform for shaping

[3] In particular, decisions can be made on compliance of legal norms and personal data security measures in force with the provisions of the Council of Europe Convention. See [Federal Law of 27 July 2006 N 152-FZ].

global AI rules and standards, so it is important for Russia to join this initiative now to have its positions considered.

Conclusions

The analysis indicates that the selected digitalization leaders affect the digital economy in two main domains: through determining conditions for activities in their domestic digital markets and participating in shaping new global standards and rules. Swift digital transformation of the Russian economy and society requires taking into account the experiences of these countries and the consequences of their influence. The analysis of the influence of the G20's digitalization leadership on the development conditions and governance of the digital economy served as a basis for policy recommendations concerning relevant measures at the national level and promotion of Russian digital agenda priorities in international institutions.

Based on the results of the study, the six main digital economy regulation areas can be divided into two groups. In the areas of digital infrastructure development, cybersecurity and data governance, there is a tendency for growing contradictions between the approaches of the U.S., the UK, Japan and partly the EU and Korea on the one hand, and Russia, China and India, on the other. In the areas of designing standards and norms for the development and application of AI, coordinated digital market regulation at the international level, and international regulation, monitoring, and supervision of global stablecoins, and issuance of CBDCs there are no serious conceptual contradictions between Russia and other BRICS members and the leading developed countries.

In the areas from the first group, coordination within BRICS should be strengthened to develop common positions and jointly promote them in the G20 and other institutions. As part of Eurasian integration, Russia should stimulate the adoption of digital economy development strategies by the EAEU partners and their maximum consistency, intensify cooperation on harmonizing digital standards, strengthen the institutional and legal foundations of the Digital Agenda, build a coordinated system for regulating the digital environment at the EAEU and national levels, and ensure sufficient funding to bridge the digital divide within and between countries. It is important to use the synergistic effect of pairing projects within the EAEU's digital agenda and the Chinese Digital Silk Road initiative in the most promising areas, such as 5G development.

Russia should also promote the idea of discussing and adopting global approaches to cybersecurity, primarily within the UN framework, and strengthen its positions within the OSCE and the Council of Europe, using relatively more favourable bilateral relations with some individual EU members. Regarding cross-border data flow governance, Russia should increase activity and the quality of its engagement to reach a multilateral consensus within the WTO negotiation process on e-commerce and intensify coordination with its traditional allies and other countries whose positions are closest to Russian ones.

As for the second group, the main recommendations are related to using the selected countries' experience when shaping Russia's own national policy. For instance, to develop an approach to large online platforms, balancing preferences for national companies and fair competition, Russian regulators could examine the EU policies. Given the experience of Russia's key BRICS partners – India and China – the five countries could coordinate positions on CBDCs and other digital assets, thus contributing to the broader goals of international financial system reform. Regarding AI technologies, given the experience of the selected countries and the EU, the Russian government should provide funding for enhancing its engagement in international cooperation and establishing international partnerships, including through interaction

with the Global Partnership on AI. Such measures will help ensure that Russia will not stay away from the emerging process of developing global principles in this area.

The proposed recommendations in certain areas should be based on a set of systemic measures. In particular, efforts to strengthen Russia's digital economy should be based on creating appropriate conditions for business digitalization, growth of the digital sector and improving opportunities for exports. To this end, the priorities of supporting the digital economy and national innovative enterprises should be linked with Russian development assistance programmes. It is advisable to strengthen state support measures for bringing domestic digital solutions to foreign markets, including through "regulatory export sandboxes," and to facilitate the creation of additional competitive advantages through international partnerships.

The implementation of these recommendations will help achieve national digital transformation goals and strengthen Russian positions in the growing global struggle for digital leadership.

References

Bank of Russia (2021) Digital Ruble Concept. Available at: https://www.cbr.ru/Content/Document/File/120239/dr_cocept.pdf (accessed 15 December 2021).

CIFAR (n.d.) Pan-Canadian AI Strategy. Available at: https://cifar.ca/ai/ (accessed 15 December 2021).

Cory N., Dascoli L. (2021) How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. *Information Technology & Innovation Foundation*, 19 July. Available at: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost (accessed 15 December 2021).

Dalmia V. P. (2021) India: Personal Data Protection Bill, 2019. *Mondaq*, 13 January. Available at: https://www.mondaq.com/india/data-protection/1024292/personal-data-protection-bill-2019#:~:text=The%20Personal%20Data%20Protection%20Bill,coming%20budget%20session%20of%202021 (accessed 15 December 2021).

EU4Digital (n.d.) Eastern Partnership. Available at: https://eufordigital.eu/discover-eu/eastern-partnership/ (accessed 15 December 2021).

European Commission (EC) (2020a) Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU. COM(2020) 591 final. Brussels, 24 September. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591 (accessed 15 December 2021).

European Commission (EC) (2020b) 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. COM(2020) 825 final. Brussels, 15 December. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72148 (accessed 15 December 2021).

European Commission (EC) (2020c) 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. Brussels, 15 December. Available at: https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf (accessed 15 December 2021).

Federal'nyj zakon ot 27 iyulya 2006 g. (red. ot 02.07.2021) "O personal'nyh dannyh" [Federal Law of 27 July 2006 N 152-FZ (as Amended on 2 July 2021) "On Personal Data"]. Available at: https://legalacts.ru/doc/152_FZ-o-personalnyh-dannyh/glava-2/statja-12/ (accessed 15 December 2021) (in Russian).

Goodman M. (2021) Advancing Data Governance in the G7. CSIS Commentary, 2 February, Center for Strategic and International Studies. Available at: https://www.csis.org/analysis/advancing-data-governance-g7 (accessed 15 December 2021).

Gov.UK (2016) National Cyber Security Strategy 2016 to 2021. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (accessed 15 December 2021).

Gov.UK (2019) AI Sector Deal. Available at: https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal (accessed 15 December 2021).

Gov.UK (2020) Telecommunications (Security) Bill. Available at: https://www.gov.uk/government/collections/telecommunications-security-bill (accessed 15 December 2021).

Gov.UK (2021a) Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy. Available at: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy (accessed 15 December 2021).

Gov.UK (2021b) Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy: Foreword From the Prime Minister. Available at: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy (accessed 15 December 2021).

Gov.UK (2021c) A New Pro-Competition Regime for Digital Markets. 20 July. Available at: https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets (accessed 15 December 2021).

Government of the Peoples' Republic of China (PRC) (2016) The 13th Five-Year Plan for Economic and Social Development of the Peoples' Republic of China 2016–2020. Available at: https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf (accessed 15 December 2021).

Government of the Peoples' Republic of China (PRC) (2017) Guó wù yuàn guān yú yìn fā xīn yī dài rén gōng zhì néng fā zhǎn guī huá de tōng zhī [Notice of the State Council on Issuing the New Generation Artificial Intelligence Development Plan]. Guofa [2017] No 35. Available at: http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (accessed 15 December 2021) (in Chinese).

Government of the Republic of Korea (2019) National Strategy for Artificial Intelligence. Available at: https://oecd.ai/en/wonk/documents/korea-national-strategy-for-ai-2019 (accessed 15 December 2021).

Government of the Russian Federation (RF) (2019) Dorozhnaya karta razvitiya «skvoznoj» cifrovoj tekhnologii «nejrotekhnologii i iskusstvennyj intellekt [Roadmap for the Development of "Overarching" Digital Technology "Neurotechnologies and Artificial Intelligence"]. Available at: https://digital.gov.ru/uploaded/files/07102019ii.pdf (accessed 15 December 2021) (in Russian).

King R. (2021) Digital Revolution: Perks of a Global Chinese CBDC. Central Banking, 17 August. Available at: https://www.centralbanking.com/central-banks/currency/7867221/digital-revolution-perks-of-a-global-chinese-cbdc (accessed 15 December 2021).

Ledger Insights (2021) China Warns on Stablecoins as Digital Yuan Users Pass 10 Million. 8 July. Available at: https://www.ledgerinsights.com/china-warns-on-stablecoins-as-digital-yuan-users-pass-10-million/ (accessed 15 December 2021).

Ministry of Foreign Affairs of the Russian Federation (RF) (2020). O pozicii Rossii na 75-j sessii General`noj Assamblei OON [On the Position of Russia at the 75th Session of the United Nations General Assembly]. 23 July. Available at: https://www.mid.ru/ru/foreign_policy/news/1437475/ (accessed 15 December 2021). (in Russian)

National Audit Office (NAO) (2021) Progress of the 2016–2021 National Cyber Security Programme. Available at: https://www.nao.org.uk/report/progress-of-the-2016-2021-national-cyber-security-programme/ (accessed 15 December 2021).

Organisation for Economic Co-operation and Development (OECD) (2019) Recommendation of the Council on Artificial Intelligence. OECD/Legal/0449. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (accessed 15 December 2021).

Organisation for Economic Co-operation and Development (OECD) (2021a) Addressing the Tax Challenges Arising From the Digitalisation of the Economy. OECD/G20 Base Erosion and Profit Shifting Project, 21 July. Available at: https://www.oecd.org/tax/beps/brochure-addressing-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-july-2021.pdf (accessed 15 December 2021).

Organisation for Economic Co-operation and Development (OECD) (2021b) Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers. OECD Trade Policy Paper No 248. Available at: https://doi.org/10.1787/ca9f974e-en.

President of the Russian Federation (RF) (2019) Ukaz Prezidenta Rossijskoj Federacii ot 10.10.2019 g. № 490 "O razvitii iskusstvennogo intellekta v Rossijskoj Federacii" [Executive Order of the President of the Russian Federation of 10 October 2019 No 490 "On the Development of Artificial Intelligence in the Russian Federation"]. Available at: http://www.kremlin.ru/acts/bank/44731 (accessed 15 December 2021). (in Russian)

President of the United States of America (2018) National Cyber Strategy of the United States of America. Available at: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed 15 December 2021).

Privacy Shield (n.d.) Available at: https://www.privacyshield.gov (accessed 15 December 2021).

Shelepov A. (2021) Obzor politiki po regulirovaniyu global'nyh stejblkoinov i cifrovyh valyut central'nyh bankov v nekotoryh stranah-chlenah "Gruppy dvadcati" [Regulating Global Stablecoins and Central Bank Digital Currencies in Selected G20 Countries]. *International Organisations Research Journal*, vol. 16, no 4. Available at: https://doi.org/10.17323/1996-7845-2021-04-09. (in Russian)

TASS (2021) Mincifry obsuzhdaet s Minoborony vydelenie chastot 3,4–3,8 GGc dlya 5G v Moskve [The Ministry of Digital Development Discusses With the Ministry of Defense the Allocation of 3.4-3.8 GHz Frequencies for 5G in Moscow. 18 October. Available at: https://tass.ru/ekonomika/12692801 (accessed 15 December 2021). (in Russian)

The White House (2021) Updated Fact Sheet: Bipartisan Infrastructure Investment and Jobs Act. Statements and Releases, 2 August. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/02/updated-fact-sheet-bipartisan-infrastructure-investment-and-jobs-act/ (accessed 15 December 2021).

Shen H. (2018) Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative. *International Journal of Communication*, vol. 12, pp. 2683–701. Available at: https://ijoc.org/index.php/ijoc/article/view/8405 (accessed 15 December 2021).

Swire S. (2021) U.K.'s Post-Brexit Strategy on Cross-Border Data Flows. *Lawfare*, 1 September. Available at: https://www.lawfareblog.com/uks-post-brexit-strategy-cross-border-data-flows (accessed 15 December 2021).

WilmerHale (2021) *China Tightens Control Over Overseas Securities Listings in Name of Data Security*. Available at: https://www.chainnews.com/articles/762892395785.htm (accessed 15 December 2021).

Xiong X., Zhang H. (2021) China Launches 3-Year Draft Plan for Cybersecurity Sector After Regulatory Actions. *Global Times*, 12 July. Available at: https://www.globaltimes.cn/page/202107/1228461.shtml (accessed 15 December 2021).